CYBERSPACE SUPERIORITY:

DOMINATING THE DIGITAL FRONTIER

by

Lieutenant Colonel William D. Bryant, USAF

A dissertation presented to the faculty of Air University in partial fulfillment of the requirements for the degree of Doctor of Philosophy

Maxwell Air Force Base, Alabama

2014

_____
Stephen E. Wright, PhD
Committee Chairman

_____
Thomas D. McCarthy, PhD, Col, USAF
Committee Member

_____
Kalu N. Kalu, PhD
Committee Member

_____
Colonel Jeffrey J. Smith
Commandant and Dean
School of Advanced Air and Space Studies

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

DISCLAIMER

The views expressed in this dissertation are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University.

BIOGRAPHY

Lt Col Bryant (BS, United States Air Force Academy; MA American Military University; MA, The George Washington University; MSS [Master of Space Systems], Air Force Institute of Technology; MAAS [Master of Airpower Art and Science], School of Advanced Air and Space Studies) is currently a student at the Air War College at Maxwell AFB, AL. Previously, he served as an operational support squadron commander, director of operations, and numerous operational and staff assignments. As a career fighter pilot, he has more than 1,500 hours in the F-16.

ABSTRACT

A combatant has cyberspace superiority when they have established an operational advantage in cyberspace to conduct operations. Cyberspace superiority can be compared to well established concepts of domain superiority in the maritime and air domains but it has unique characteristics. All of the domains have concepts of superiority but they differ in the importance of local versus universal domain superiority. Local cyberspace superiority is much more important and easier to achieve for cyberspace operators. Cyberspace superiority can be measured by utilizing a weighted preference methodology that considers offensive objectives, the importance of those objectives, defensive success, the importance of defended systems, and the relative importance of cyberspace to each combatant. Cyberspace superiority will tend to be very local and transitory with a rapid degradation once an attacker is identified by defenders. These characteristics were verified by a comparison of eight case studies where cyberspace superiority was always local and was only persistent in the one case study where the attack itself was hidden from the defender. The case studies also illustrated that the offense does not have an overwhelming advantage as the in 50% of the cases, the defenders maintained cyberspace superiority despite the inherent advantages of the offense where in cyberspace the attacker is hidden and the defender out in the open. The case studies also clearly illustrate that the accomplishment of cyberspace superiority brings significant advantage to a combatant at the strategic, operational, and tactical levels of war.

1 – INTRODUCTION

The importance of cyberspace continues to grow in the modern world. Now it is not just the box under the desk called a "computer" that is part of cyberspace. We are connecting our cars, phones, kitchen appliances, and even toilets into the Global Information Grid or GIG. These connections allow increases in functionality and productivity unimaginable in the realm of science fiction a few years ago. Today's iPhone makes a "Star Trek" communicator look like a ridiculously simple and crude device, but the iPhone is real. However, just like a "Star Trek" ship's computer run amok, our devices may be working against us.

There is a dark side to this ever-increasing connectivity and functionality. Our iPhone can be spying on us and reporting our every move to a foreign intelligence service, our car might be reporting our location to an enemy, and malicious hackers can take over even our humble toilet to humiliate us.[1] Action from cyberspace is not limited only to malicious pranks. Hackers have demonstrated the ability to send potentially lethal commands to common cars such as the Toyota Prius. One pair of enterprising hackers has demonstrated the capability to blast the horn uncontrollably, "make pathological liars out of speedometers and odometers," spoof the GPS, and even violently jerk a Prius' steering at any speed, threatening a potentially lethal collision.[2] These

[1] Trevor Mogg, "Smart Toilet Security Flaw Could Result in Nasty Surprise," *Fox News*, 5 August 2013. http://www.foxnews.com/tech/2013/08/05/smart-toilet-security-flaw/.
[2] Andy Greenberg, "Hackers Reveal Nasty New Car Attacks—With Me Behind the Wheel (Video)," *Forbes*, 24 July 2013. http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/

threats and vulnerabilities become even more magnified as you look at cyberspace systems on the municipal or national level.

Cyberspace is increasingly becoming an arena for nation state conflict. If a nation were to drop a bomb on an enemy power plant, the target nation would clearly consider it an act of war. If the same nation dropped a "logic bomb" through cyberspace causing the same amount of damage to the power grid, that is also war. The delivery method does not change the physical effect of the attack. Analysts are increasingly accepting cyberspace as a domain where combatants fight, much like the domains of land, maritime, air, and space. According to former National Security Council Director for Cyber Security Gregory Rattray, a goal of U.S. national strategy is to gain control of cyberspace.[3] The nature of warfare has not changed, but now there is a new field to fight on, much like when aircraft first opened up the air domain to warfare in the early 1900s. If cyberspace is a domain, what does that mean? What is the basic character of this new domain?

Cyberspace is difficult to grasp intuitively because we cannot easily see it with our eyes. According to Professor Chris Demchak, "…orchestrating a national security response to cybered threats is hard because cyberspace is *hard to see physically* in any case, but especially so now as it is deeply embedded in normal societal functions."[4] Cyberspace is not the only domain that is invisible to the eye; an observer cannot see the air domain although he can see the aircraft moving through it unlike cyberspace packets

[3] Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, DC: Potomac Books, 2009), 255.
[4] Chris C. Demchak, *Wars of Disruption and Resilience* (Athens: The University of Georgia Press, 2011), 176.

of information. The difficulty in visualizing cyberspace makes careful definition of the domain even more important.

Connections between computing devices create cyberspace. An isolated computer sitting on a desk is no more part of the cyberspace domain than a ship sitting in dry dock is part of the maritime domain. The connections are what matter. The Joint Staff has defined cyberspace as, "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[5] While this definition has achieved wide acceptance, there are still a few contentious issues.

One point of the definition that analysts still debate is whether or not to include the electromagnetic spectrum. As analysts first developed cyberspace as a concept, some policy makers included the electromagnetic spectrum as cyberspace's "maneuver space."[6] However, according to Thomas McCarthy, over time the definition has narrowed "down to the physical network infrastructure used for transmitting and storing information."[7] Sean Butler gave the principal reason behind this narrowing when he stated that,

> The ability to process, store, and exchange large amounts of information rapidly, using automated systems, is the defining characteristic of cyberspace—the physical methods are superficial. In fact, its logical or virtual nature, rather than its physical mechanisms, sets cyberspace apart from other domains.[8]

---

[5] Joint Chiefs of Staff, Joint Operations, Vol. 3-13, *Information Operations*, 2012, II-9.
[6] Michael W. Wynne, "Flying and Fighting in Cyberspace," *Air Space Power Journal*, Volume 21, no. 1 (2007): 6.
[7] Thomas David McCarthy, "Traveling Domain Theory: A Comparative Approach for Cyberspace Theory Development" (PhD diss., Fletcher School of Law and Diplomacy, 2012), 56.
[8] Sean C. Butler, "Refocusing Cyber Warfare Thought," *Air Space Power Journal* Volume 27, no. 1 (January – February 2013): 50.

I find McCarthy's argument compelling and so will utilize the narrower Joint Staff definition from *Information Operations* for cyberspace, which does not try to include the entire electromagnetic spectrum.[9] I present a much more detailed analysis of the characteristics of the cyberspace domain in chapter 3. Now that we have a definition of cyberspace, is freedom of action within that domain significant?

If the cyberspace domain is a key component of modern warfare, then freedom of action within that domain is important. According to Air Force Doctrine Document (AFDD) 3-12,

> Freedom of action in the cyberspace domain enables our command, control, communication, computers, intelligence, surveillance, and reconnaissance capabilities. Our modern defenses, industrial base, and global commerce, as well as that of our nation's enemies, depend on free use of land, sea, air, space, and cyberspace. Leverage in cyberspace affords influence and control across all other domains. This leverage increases our forces' access, speed, reach, stealth, and precision.[10]

In other domains, and especially in the air and maritime domains, analysts refer to this freedom of action as superiority.

The United States Air Force presents a clear definition of cyberspace superiority in Air Force doctrine. According to AFDD 3-12, cyberspace superiority is, "The operational advantage in, through, and from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference."[11] This definition is the one

[9] There are numerous definitions of cyberspace, Daniel Kuehl gives 14 in a single article in Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem." in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, DC: Potomac Books, 2009), 26-27. What is common across the majority of the definitions is the idea of communication via connected computing devices. I use the Joint Staff definition as it is well known and I find it to be among the most complete without overreaching into the electromagnetic spectrum.
[10] Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations. Change 1*, 15 July 2010, ii.
[11] AFDD 3-12, *Cyberspace Operations. Change 1*, 2.

I will use of cyberspace superiority within this project and it is important to note that cyberspace superiority has both an offensive and defensive component. Understanding this is critical to this project and AFDD 3-12 goes on to provide more context and expand on the simple definition.

> Cyberspace superiority may be localized in time and space, or it may be broad and enduring. The concept of cyberspace superiority hinges on the idea of preventing prohibitive interference to joint forces from opposing forces, which would prevent joint forces from creating their desired effects. "Supremacy" prevents effective interference, which does not mean that no interference exists, but that any attempted interference can be countered or should be so negligible as to have little or no effect on operations. While "supremacy" is most desirable, it may not be operationally feasible. Cyberspace superiority, even local or mission-specific cyberspace superiority, may provide sufficient freedom of action to create desired effects. Therefore, commanders should determine the minimum level of control required to accomplish their mission and assign the appropriate level of effort.[12]

I will explore a number of important elements in this definition. The first element encompasses the different levels of cyberspace superiority.

There is a wide range of possibilities on how much advantage a combatant can have in a given domain. Note that in the AFDD 3-12 section quoted previously, there are at least two different words used to discuss friendly freedom of action, "superiority," and "supremacy." There are also a large number of terms that different authors and thinkers have applied to advantage in a domain that includes command, control, supremacy, and superiority. Because different authors often use these terms to mean different things, it can be very confusing when comparing multiple works. "Sea control," "command of the sea," "maritime superiority," and "control of sea communications" are all similar

[12] AFDD 3-12, *Cyberspace Operations. Change 1*, 2.

concepts, but there is no generally accepted hierarchy or understanding of how each term relates to the others. Accordingly, in this project I utilize a single term of cyberspace superiority, while acknowledging that there will be different levels of cyberspace superiority from near parity among the combatants, to complete domination of all of cyberspace by one combatant. In many of the quotations from other authors throughout this project, they use other terms such as "command of the air" or "sea superiority" and I have not altered them. I consider each of them to refer to domain superiority in their domain, with the addition that sometimes they imply greater or lesser domain superiority as in AFDD 3-12, which places cyberspace supremacy over cyberspace superiority. The range of strength of superiority that a combatant can achieve brings up the related question of how much superiority a combatant needs or should seek.

A combatant should be seeking just enough cyberspace superiority to achieve his or her objectives, because seeking too much superiority can be counterproductive and prevent the attainment of strategic or operational objectives. For a combatant to pursue domain superiority requires resources that he or she could have applied to other important objectives. In addition, if a combatant seeks too high a level of superiority, there can be significantly diminishing returns for the increased resources put towards solving the problem. For example, in the air domain a combatant may be able to reduce an enemy Integrated Air Defense System (IADS) to 50% effectiveness at a reasonable level of effort, but to get to 99% degradation will normally be cost prohibitive. Temporary, local superiority may be sufficient if that is all that is required to accomplish the mission. For example, when the Israeli Air Force bombed the Iraqi nuclear reactor, they did not seek air supremacy or even air superiority over all of Iraq; they simply wanted air superiority

over the target and the ingress and egress corridors for just long enough to destroy the reactor. The Israelis were very successful by only seeking just enough superiority to accomplish their mission; had they attempted to gain total air supremacy, they would not have been able to, and would not have been able to destroy the reactor as well. On the other hand, some analysts think that even limited cyberspace superiority is not a useful concept or goal for military forces.

Analysts have a wide range of opinions on the utility of cyberspace superiority as a concept. Martin Libicki is a well-known cyberspace analyst who is rather blunt when he states that, "…the question of cybersupremacy is meaningless and, as such, is not a proper goal for operational cyberwarriors."[13] Owens, Dam, and Lin are slightly more circumspect and see some utility for developing capabilities, but still say that conflict in cyberspace will be very different from in the land, air, and maritime domains, which will make enduring dominance of cyberspace by the United States unrealistic.[14] Cyberspace analyst Jeffrey Carr states that the tendency of U.S. military forces to attempt to control the domains they operate in is a problem for the United States as no nation can dominate or control cyberspace.[15] Carr is afraid that the United States will pour resources into seeking an objective that is not attainable. Professor David Lonsdale concurs with Carr that a high level of cyberspace superiority is not attainable. Lonsdale looks at Douhet's definition of command of the air and states that an equivalent command of cyberspace is

[13] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), 141.
[14] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009), 39.
[15] Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Beijing: O'Reilly Media, 2011), Kindle location 4089, chap. 11.

impossible and even undesirable, as it would require denying an enemy effective use of their information assets.[16] Not all analysts agree that there is no value to the concept of cyberspace superiority; some see it as a useful concept that requires modification when applied to the new cyberspace domain.

What these objections highlight is that cyberspace is not like the other domains, which will make gaining superiority look very different, and the character of the superiority gained may be different as well. This difference in character does not release the cyberspace warrior from attempting to control his or her domain. According to well known strategic theorist Colin Gray,

> To make advantageous use of an army, navy, air force, space force, and information force, it is necessary as a prerequisite to seek out and defeat the geographically similar forces of the enemy. If use of the sea is vital to us, in consequence it is vital to an enemy that he should be able to contest our ability to use the sea. The same strategic logic applies to the air, to orbital space, and to cyberspace. The technologies, tactics, and operational aims must vary with what is feasible in each unique geographical environment: the strategic logic, however, is uniform.[17]

Gray's strategic logic will drive cyberspace operators to attempt to control the cyberspace domain even if it is difficult. We should not simply ignore cyberspace superiority, we should wrestle with it to determine whether or not there is utility for strategists and planners in the concept.

One aspect of this project is to examine how the technologies, tactics, and operational aims of a combatant will function in the pursuit of cyberspace superiority. Libicki thinks cyberspace superiority is not worth thinking about, and most analysts

---

[16] David J. Lonsdale, *The Nature of War in the Information Age* (London: Frank Cass, 2004), 184.
[17] Colin S. Gray, *Modern Strategy* (Oxford: Oxford University Press, 1999), 209.

seem, at best, uncomfortable with the concept. However, the United States Air Force puts it into official doctrine as a key concept. Who is correct? Does cyberspace superiority even exist? Is it a useful concept? All of these questions lead into the research question for this project.

Does a nation that achieves a level of cyberspace superiority during a conflict gain a significant operational advantage?

The operational advantage produced by cyberspace superiority includes cyberspace operations in a supporting role to land, maritime, air or space forces, as well as cyberspace operations intended directly to produce effects through strategic information warfare. This research question brings up several other questions that I will need to deal with before I can answer the overarching question.

The first supporting question is whether domain superiority is a local or universal concept. In the more familiar air domain, combatants often implement air superiority through combat air patrols, or CAPs, where fighter aircraft hold a position and deny that space to the enemy. However, a single flight of aircraft cannot fly to their assigned CAP, "plant the flag" and fly home having established air superiority over the entire theater of operations. They have only established air superiority in the area of the domain that their sensors and weapons can reach and only for as long as they are in their CAP. Nevertheless, the fact that they have established superiority in their local part of the air domain, also affects the overall superiority in the theater air domain, as the enemy now cannot utilize the airspace occupied by the CAP without fighting for it. This example highlights one of the key supporting questions that I will explore in this project. What is the relationship is between local and universal superiority in the cyberspace domain? I

will examine how the local and universal levels of domain superiority interact among the physical domains to find elements and strands that I can apply to the cyberspace domain. The simple example of a CAP in the air domain also highlights another issue.

The second supporting question is how persistent domain superiority will be. When the aircraft return to base, what happens to the air superiority that the combatant gained? Does it continue and persist? In the case of the CAP, once the aircraft return to base, the enemy can utilize the airspace just as easily as before the aircraft set up the CAP, so there is no longer superiority in that localized area. Accordingly, the combatant will have to rotate aircraft through the CAP so that there are always fighters on station if he or she desires persistent superiority. What does persistence look like in the cyberspace domain? After all, if the persistence of superiority in a domain is zero, then there cannot be superiority in that domain. Does the great speed of action in the cyberspace domain result in persistence so short that it makes cyberspace superiority not worth pursuing? Looking at the persistence of cyberspace superiority over time brings up the final issue.

To examine the persistence of cyberspace superiority over time, I will need to develop some way of measuring cyberspace superiority. Simply comparing the force structures of the two sides will not tell you definitively who has, or is likely to gain, superiority. If an analyst looked only at the aircraft and systems possessed by Israel and Syria before the Bekaa Valley air campaign of 1982, it would have given no indication of the extremely one-sided air superiority subsequently gained by the Israelis. However, there are useful metrics that combatants routinely utilize to measure air superiority. What percentages of friendly strike aircraft are successfully attacking their targets? How many enemy aircraft are getting through and hitting friendly targets? Which side is losing more

aircraft? Often, the indicators will be mixed and hard to read during a campaign. In a few cases, the superiority is obvious, as when the Iraqis completely ceded the air domain and buried their fighters in the sand to try to preserve them for the future. Generally, measurement of superiority in the cyberspace domain is not so simple.

Measurement of the level of superiority in the cyberspace domain is extremely difficult. The cyberspace domain is less tangible than the physical domains and it is harder to count and compare cyberspace weapons versus aircraft, ships, or infantry divisions. However, many of the same concepts will apply. What percentage of friendly cyberspace strikes got through enemy defenses? How successfully are friendly defenses at holding off enemy cyberspace attacks? These are the key questions that will form the foundation of a methodology of measuring cyberspace superiority that I will develop in this project. As with the questions on local and universal issues, or persistence, I will first turn to the other physical domains to see what lessons I can pull out that may apply to the cyberspace domain. After I have dealt with these questions, I will be able to answer the main research question.

My hypothesis is that a meaningful level of cyberspace superiority will produce a significant operational advantage, such that:

If a nation achieves cyberspace superiority during a conflict, then it gains a significant operational advantage.

Following Professor Stephen Van Evera's political science theory methodology, I depict my research hypothesis below in figure 1.[18]

[18] Stephen Van Evera, *Guide to Methods for Students of Political Science* (Ithaca, NY: Cornell University Press, 1997), 7-17.

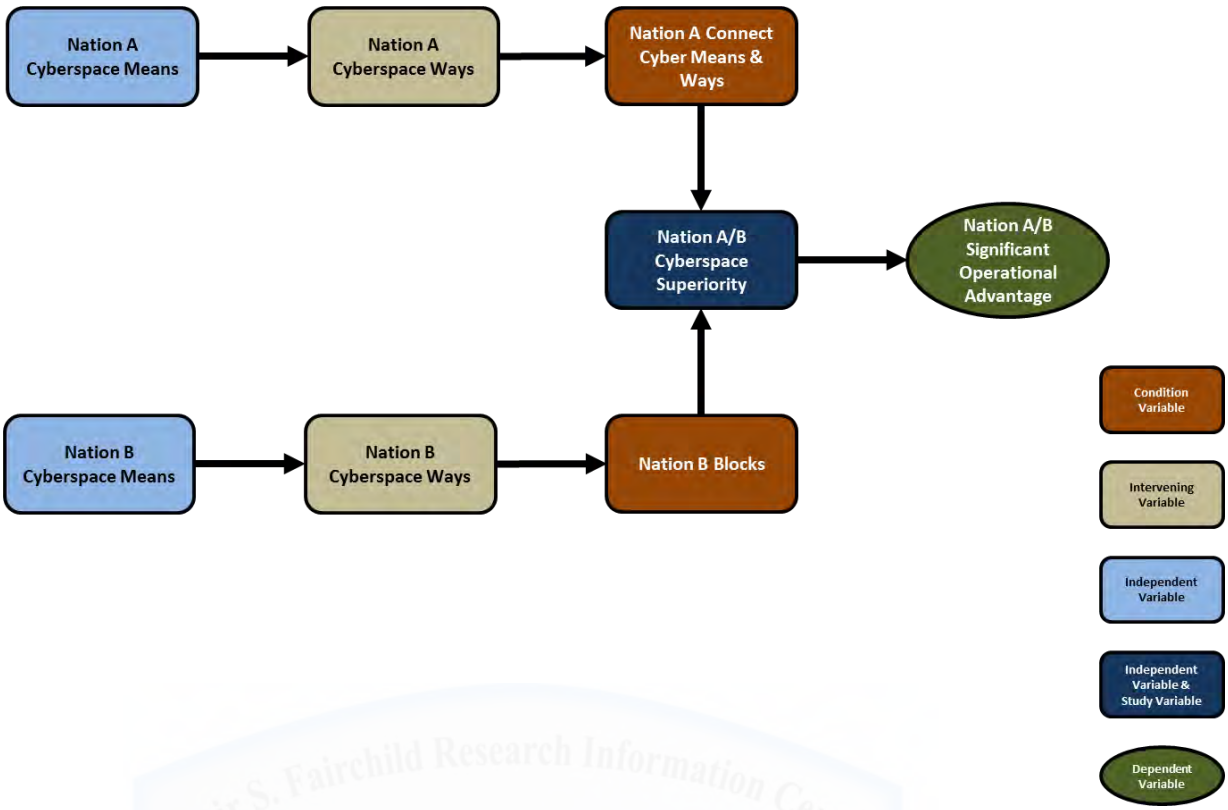

Figure 1 – Research Hypothesis
Source: Author's Original Work Derived from Stephen Van Evera, *Guide to Methods for Students of Political Science* (Ithaca, NY: Cornell University Press, 1997), 7-17.

The dependent variable is who gains significant operational advantage, which is caused by the independent and study variable of cyberspace superiority. There are also two condition variables that determine the study variable. The first condition variable is nation A's connection of its cyberspace means and ways. This condition variable is generated by the independent variable of nation A's cyberspace means, with an intervening variable of nation A's cyberspace ways. There are always two parties to a conflict and nation B has its own condition variable that affects who achieves cyberspace superiority. Nation B's cyberspace means is the independent variable with nation B's

cyberspace ways as an intervening variable. This structure clearly lays out the relationships among the variables I posit in this study.

To answer the research question and test this hypothesis, I will start by examining the elements of domain superiority and persistence of superiority from other domains in chapter 2. I will also develop a general model that links universal and local domain superiority and apply it to the land, maritime, and air domains. Then, in chapter 3, I will examine the characteristics of cyberspace to develop the elements of domain superiority as they apply to cyberspace to include a measurement concept for cyberspace superiority. I will also apply the general model linking universal and local domain superiority to cyberspace. Chapter 4 will be dedicated to developing a measurement system for cyberspace superiority. After I have developed the measurement system, I will apply it to analyze three main case studies against the limited historical cases currently available in chapter 5. Having demonstrated how cyberspace superiority contributes to military operations, the final chapter will summarize this work, the conclusions, and implications for the future and for future analysis. I will start by examining what elements of domain superiority I can pull from the other physical domains.

2 – ELEMENTS OF DOMAIN SUPERIORITY FROM OTHER DOMAINS

Examining the other domains will yield critical concepts and elements that I can apply to the cyberspace domain. An idea of how cyberspace superiority operates does not have to start *ex nihilo*, or from nothing; rather, it should leverage the large body of work that analysts have already developed in other domains. I can pull out elements from the work of theorists in other domains to determine what elements should likely be included in the cyberspace domain. I can do this for both concepts of how superiority in the domain operates, and how it is measured. First, I will define what a domain is, and which ones I will examine in detail in this study.

For this project, a domain is a distinctive sphere of operations bounded by unique characteristics. There are many definitions of the term "domain." McCarthy identified ten in a single dictionary but narrowed the list to the three most applicable, which include:

1. A region distinctively marked by some distinctive feature
2. A sphere of knowledge, influence, or activity
3. A territory over which dominion is exercised[1]

All three of these apply to the traditionally recognized domains in warfare of land, maritime, air, space, and now cyberspace. Combatants have long fought over all of these domains.

Each of the domains has been the focus of struggles for control. Since the dawn of time, men fought for control of the land domain. As soon as men took to the water,

[1] The definitions are from The Merriam-Webster online dictionary quoted in McCarthy, "Traveling Domain Theory," 47.

they fought for control of that domain as well. The Egyptians, Minoans and Mycenaeans were building warships to contest the maritime domain in 1500 B.C.E.[2] It also was not long after the first powered flight that the Europeans fought for superiority in the air domain during World War I. The struggle in the space domain has taken a unique form, due to the characteristics of that domain, but there is no shortage of ideas and programs to seek domain superiority in space as well. One thing that has been common across these domains is that military forces have sought superiority in all of them.

Military forces tend to first seek to dominate their domain before they attempt to affect other domains. This tendency to seek dominance in their domain first is perfectly natural as forces focused on a specific domain such as land, maritime, or air spend most of their time thinking about and operating in that domain. Maritime and air forces generally see establishing control of their domain as a prerequisite to accomplishing other cross-domain missions, while land forces tend to see their domain as having primacy over all the others. Who is right in the continuing debates over missions is not relevant to this discussion; each domain specific warfighter is correct that they cannot operate effectively without at least some control over their domain and, thus, cannot provide anything to other domains before establishing enough superiority in their own domain to operate. McCarthy looked at superiority across multiple domains and multiple theorists to determine that, "*The pursuit of domain control is the primary function of domain-centric*

[2] R.G. Grant, *Battle at Sea: 3,000 Years of Naval Warfare* (London: Dorling Kindersley, 2008) 24.

forces."[3] Accordingly, I will examine those domain control theories to determine their relevance to cyberspace superiority.

While I will examine domain superiority theories from the land, maritime, and air domains, I will not examine space superiority theory for two reasons. First, the space domain is immature and there has not been enough conflict in the domain to clarify the lessons on superiority from that domain. Secondly, there is no accepted theory of how the space domain operates as a medium of war. Each of the U.S. service war colleges study Clausewitz, Sun Tzu, Jomini and others from the land domain, A. T. Mahan and Julian Corbett in the maritime domain, and Giulio Douhet and Billy Mitchell in the air domain. There are no space theorists with comparable, widely accepted theoretical works. Accordingly, I will focus on examining the other three domains.

To organize the discussion of the land, maritime and air domains, I will examine six categories in each domain. The overall purpose of this examination is to determine what elements of domain control in each of the three physical domains might apply to the cyberspace domain. First, I will examine the physical rules, geography, and distinguishing characteristics of the domain. Next, I will examine whether theorists consider the offensive or defensive generally to have the advantage in the domain. After examining the balance between offense and defense in each domain, I will turn to the third area of how a combatant gains superiority in that domain. The next element is how a combatant can utilize superiority in the domain once gained, and the fifth is whether the combatant can expect superiority to be persistent or temporary in that domain. Finally, I

[3] McCarthy, "Traveling Domain Theory," 187.

will examine what measurement concepts analysts have utilized in the domain. However, before turning to the specific domains it will be helpful to examine a generic model of gaining and utilizing domain superiority.

I can build a model of generic domain superiority by starting with the interaction between universal and local superiority. Recalling that domain superiority is the ability of a combatant to conduct operations without prohibitive interference, a combatant will experience this superiority at the local level. I define local as within a given unit's area of influence, which will of course vary widely depending on the domain and type of unit. For example, a strategic SAM system may influence an area covering hundreds of square miles, while a rifle company will have a much smaller area of influence. Beyond the differences extant in different unit's capabilities, theorists in the domains I will discuss have had differing opinions on whether domain superiority in their domain was local or universal.

I posit that a combatant will experience domain superiority at the local level, but that the forces available to contest superiority will often be determined at the universal level. For example, if nation A has 100 multi-role fighters and nation B has only 10, it is sensible to assume that at the universal level nation A has a reasonable level of air superiority. However, if one of nation A's fighter pilots finds him or herself alone in the same piece of sky as eight of nation B's fighters, it is unlikely that universal superiority will matter much in determining whether the lone nation A pilot is going to experience "prohibitive interference." As such, my general model of gaining and utilizing domain superiority looks like figure 2.

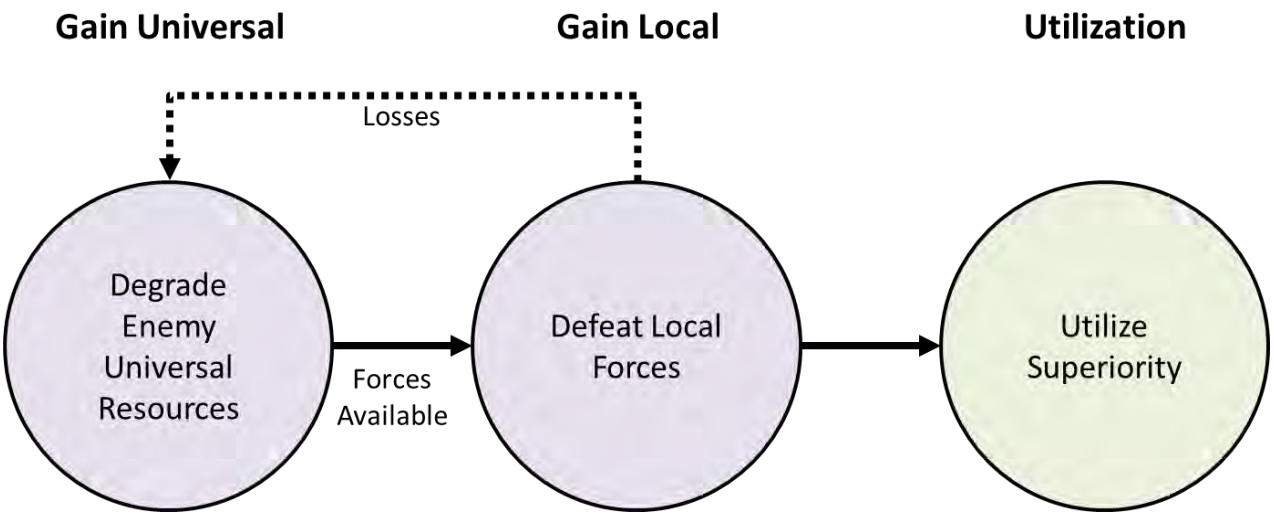

Figure 2 – General Model of Gaining and Utilizing Domain Superiority
Source: Author's Original Work

As the model indicates, there is an interaction between the universal and local levels. The universal level determines what pool of resources is available to produce local forces, and any losses at the local level affect the pool of universal resources. Of course, depending on the domain, resources may not be able to move easily from one local area to another. Once local forces have been defeated sufficiently, a combatant can then utilize the superiority gained in order to accomplish objectives designed to move the combatant closer to his or her desired goal or end state. The characteristics and current technology of each domain will alter the details of this general model, which lays out domain superiority from the perspective of only one combatant.

This first model only captures the process of gaining and utilizing domain superiority for one combatant; the enemy is also attempting to gain domain superiority at the same time. The enemy's attempt to gain superiority may mirror what a combatant is trying to do, or may be very different if the enemy has a different end state or a different method of connecting his or her means, ways, and ends. This first model will also

change in the different domains based on their characteristics. One factor that this model needs to account for in the different domains is the distinction between the offensive and defensive sides of domain superiority that domains exhibit in varying degrees.

Differences between the offensive and defensive sides of the struggle for domain superiority will be particularly important with the air and cyberspace domains as they have the greatest amount of dissimilarity between offensive and defensive forces. An infantryman, tank, destroyer or submarine all can easily execute either offensive or defensive missions. In the air domain, only multi-role fighters easily perform both missions, while bombers and cruise missiles can only effectively execute offensive missions. Surface to air missiles, on the other hand, are generally only capable of performing defensive missions.[4] This split is even greater in the cyberspace domain, with a defensive firewall having a very different character than an offensive worm or virus. These differences significantly affect the struggle for cyberspace superiority and I expanded the model in figure 3 to show that an attacker is also defending against enemy attacks at the same time he is attacking.

[4] SAMs are generally defensive weapons; but one exception to this tendency is if their range is so great that their effective range extends well into enemy territory. If a combatant could shoot down any aircraft flying in enemy territory with long range SAMs that would constitute an offensive use of SAMs no different from shooting down enemy aircraft with offensive fighter patrols. While theoretically possible, at the current time this situation is uncommon.

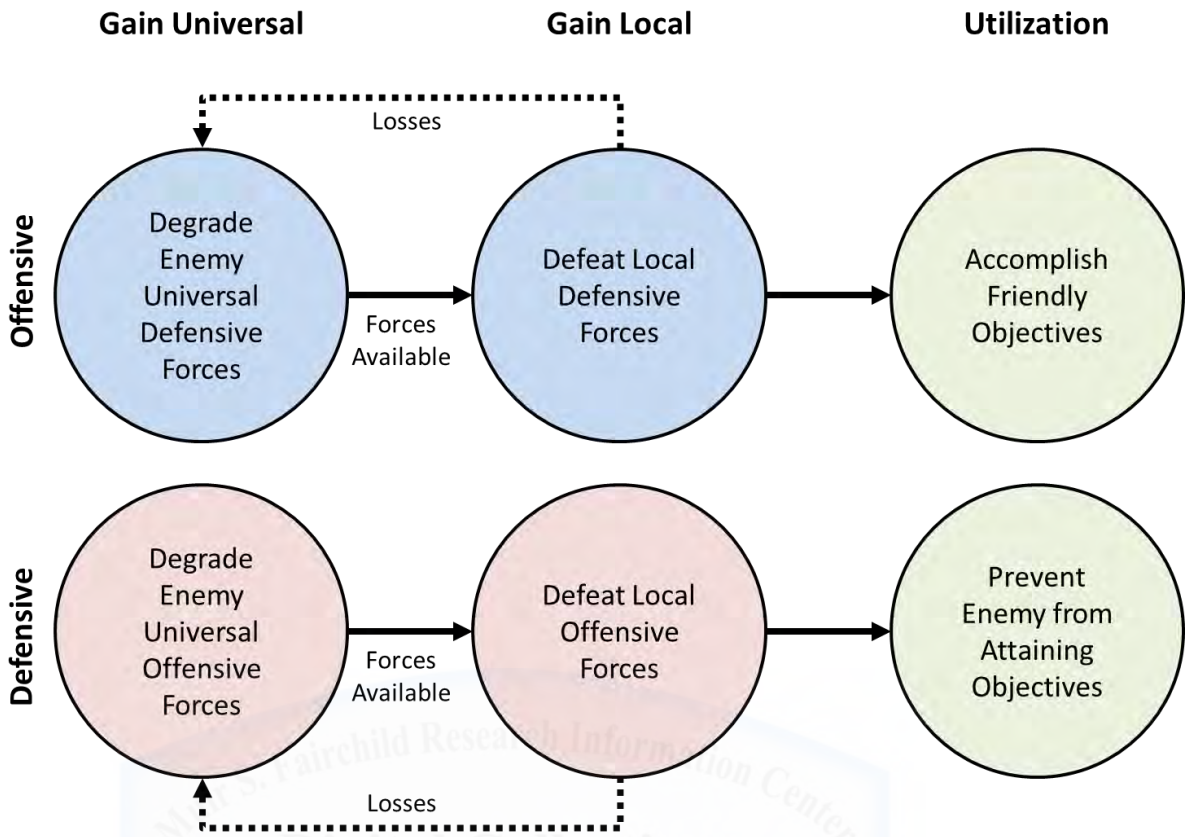

Figure 3 – Generic Model of Domain Superiority Split into Offensive and Defensive
Source: Author's Original Work

The different characteristics of the various domains will cause this model to change somewhat for each domain. First, in some domains, the forces used for offensive and defensive actions are the same; and so the blue and red offensive and defensive circles under gaining universal superiority collapse back down to a single purple circle as in figure 1. In the land and maritime domains, there is so much overlap that they will collapse completely, while in the air domain there will be some, but not complete, overlap. In the cyberspace domain, there will be no overlap as defensive and offensive weapons are completely different. However, there can be overlap in the use of superiority on the far right of figure 2.

Changes in the characteristics of the domains can also alter the amount of overlap between the offensive and defensive in utilization of domain superiority. The land and maritime domains exhibit this case as both the attacker and defender are trying to control terrain or sea lines of communication. In the air and cyberspace domains, combatants utilize offensive and defensive superiority in substantially different ways, as I will discuss in the sections on gaining superiority in those domains. Beyond the amount of overlap in utilization of forces and superiority, I will also capture the relative importance of universal and local domain superiority.

The final area of significant difference between the domains is in how important the universal versus local levels are in gaining domain superiority. In the subsequent figures specific to the domains, I will illustrate this difference by the size of the universal and local circles in the figures. I determine the size by three factors. The first is how easy it is to move forces in the domain from one local area to another, the second is how much overlap there is between offensive and defensive forces, and the third is the vulnerability of those forces to attack or degradation. As an extreme example, consider a theoretical domain where a combatant could move forces instantaneously to any local area, any force element could accomplish offensive or defensive missions equally well, and forces were easy to attack at the universal level. In this case, the universal level would completely dominate and the local level would be unimportant. If, on the other hand, there was no ability to move forces from one local area to another, offensive and defensive forces were unique and not interchangeable, and universal forces were extremely difficult to attack until they became involved in local engagements, then the local level of superiority would dominate. Of course, none of the domains is at either

extreme, but I will demonstrate wide variation with the maritime domain being the most universal and the cyberspace domain being the most local. Now that I have established a generic model of how a combatant can gain and utilize domain superiority, I will apply it to the land, maritime and air domains within a broader discussion of their characteristics. I will start by examining the land domain.

Land Domain

Geography and Characteristics of the Land Domain

The land domain is the one most unlike cyberspace. The land domain is physical, tangible, and the easiest to grasp intuitively. The most important element of superiority in the land domain is control of the land itself and the resource extraction capabilities that brings, which combatants most often implement with "boots on the ground." The cyberspace domain is radically different in each of these areas; however, there are common elements that make it worthwhile to consider the land domain before moving onto some of the more similar domains such as maritime or air. Some of these commonalities include the interface between the local and universal levels of superiority as well as the interaction between combatants as they each strive to defeat the other. The differences between the land and cyberspace domains are significant enough that it is uncommon for theorists to think in terms of land superiority at all.

It is rare to hear a discussion of "land superiority" or even "control of the land domain." Instead, land theorists have historically focused on winning battles and wars, which usually also gave control of the land or "land superiority." Since combat in the land domain came first, there is also a tendency, especially acute in earlier authors, to

consider land combat as the totality, or at least the principal point, of warfare. This narrow view is very natural given the geography of the land domain.

Land domain combatants have a very specific view of control circumscribed by their geography. Naval officer and strategist J. C. Wylie noted that, "Where the sailor or airman think in terms of an entire world, the soldier at work thinks in terms of theaters, in terms of campaigns, or in terms of battles."[5] The boundaries of a soldier's world are the physical realities of his environment. Mountains, rivers, hills, and forests shape his world and dramatically affect the struggle for superiority on land. In addition, these features greatly influence which forces have the greatest efficacy.

The geographical features in the land domain determine which forces are most effective in a specific area. For example, in classical Greek warfare, heavy infantry hoplites ruled supreme on flat unbroken terrain, but hoplites could not compete with missile troops in mountainous or heavily wooded terrain such as on the island of Sphacteria where a large number of Spartan hoplites were unexpectedly defeated.[6] This advantage of light over heavy forces when they are in mountainous or urban terrain is still true today where light infantry has significant advantages over armored forces. Conversely, in the open, the advantage goes to the heavy armor force. The geographical features in the land domain also influence how land forces look at achieving objectives.

Land forces are reliant on protecting their lines of communication and supply, which normally forces them to take a sequential approach to achieving objectives. For

---

[5] J. C. Wylie, *Military Strategy: A General Theory of Power Control* (New Brunswick, N.J.: Rutgers University Press, 1967), 49.
[6] Robert B. Strassler ed., *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*, (New York: Touchstone, 1996), 240.

example, if a combatant wanted to occupy the enemy capital, he would have to deal with each of the obstacles in front of him sequentially. The attacker has to cross the river in front of him, defeat the army defending the capital, and then seize the city. A combatant must complete each of those steps in order; attempting to jump straight to laying siege to the city without defeating the enemy army would open him up to an attack from the rear and the loss of his supply lines. The characteristics of the land domain also affect whether the offense or defense has primacy within the domain.

Offensive or Defensive Primacy in the Land Domain

As noted by Gray, the advantage for offense or defense in a domain is dependent upon the "tactical-technical logic" of that domain.[7] Since technology and tactics change over time, the advantage for the offense or defense can also change over time in a given domain. The advantage can shift due to technological development such as when the invention of rapid firing breech loading rifles shifted the advantage in land warfare towards the defensive. Sometimes, tactical innovations are required before the technical innovations have major impact. For example, the invention of the tank did not completely change warfare until the Germans connected it to the tactical innovations of *Blitzkrieg*.[8] The current state of the tactical-technical logic of the land domain gives the advantage to the defender.

[7] Gray, *Modern Strategy*, 110.

[8] The French *Mitrailleuse* provides another example of poor tactical doctrine hampering technical innovation. The French *Mitrailleuse* was a primitive form of machine gun that had minimal impact on the Franco-Prussian War of 1870 because it was treated as artillery by officers who had no idea how to use it effectively. The *Mitrailleuse* could have shifted the balance towards the defensive, much as later machine guns did, but it did not change the balance in 1870 due to poor tactical doctrine.

In the modern era of land warfare, it has normally been the case that the defender has had the advantage if the forces were roughly comparable. Thus, it has become almost a military truism that attackers should have a three to one advantage over defenders if they are to be successful. Gray explains the advantage of the defensive in land warfare by noting that on land, the attacking side has to expose itself to move forward and attack, while the defender can remain hidden or under cover while firing on the attacking force.[9] While it is possible that the general ability of a defending force to hide more effectively than an attacking force could change with improved sensors, given the current state of technology it seems unlikely.[10] With present technology and tactics, the defense has an advantage in land combat that an attacker has to overcome before gaining superiority.

Method of Gaining Land Superiority

Physical presence with forces in a local area of the domain is the key to establishing superiority in the land domain. Wylie gave one of the simplest and most compelling concepts of land control or superiority when he said, "*The ultimate determinant in war is the man on the scene with a gun.* This man is the final power in war. He is control."[11] Infantry or police forces, which have heavier firepower on call as needed, have most often established this control. The larger and more important issue is how an attacker can get possession of the contested terrain in the first place.

---

[9] Gray, *Modern Strategy*, 214.
[10] The revolution in military affairs or RMA promised to change the ability of a defending force to hide through a combination of ubiquitous sensors and networked communications and thus largely dispense of Clausewitz's famous fog of war. The results in actual combat have been disappointing; it is possible that future technological innovations will produce complete awareness for an attacker, but it seems unlikely in the near term.
[11] Wylie, *Military Strategy*, 85.

The most common way of establishing control over terrain throughout history has been to defeat the enemy army in battle. Strategic theorist Carl von Clausewitz expected that defeating the enemy army would normally be a prerequisite for control and saw control of terrain as a consequence of that victory. Only in unusual cases did he expect that a force should occupy land before defeating the enemy army.[12] Most campaigns from antiquity to Operation IRAQI FREEDOM follow this model where a combatant neutralizes enemy ground forces first, and then occupies and controls territory. One of the reasons why this pattern seems to hold is the advantage a concentrated force has over a dispersed force. A concentrated force can bring all of its combat power to focus on a single point, where a dispersed force can only utilize a fraction of its power at any one location. However, a force cannot always remain concentrated because to control terrain effectively, the force must usually disperse. Therefore, land forces normally stay concentrated until the enemy army has been defeated, and then disperse to control terrain. In addition, defeat of the enemy army will not always be required as an undefeated enemy army may withdraw and cede land superiority over an area.

Another way to gain control over terrain is for the enemy to choose to give you that control through some sort of settlement. Clausewitz did not state that battle was the only possible way to gain your objectives; he identified that occupying a "lightly held or undefended province," or changing the political environment by gaining new allies or disrupting the enemy's alliances can serve as a "short cut on the road to peace."[13] If the objective of the war was to gain territory, there is still need for Wylie's "man on the

[12] Carl von Clausewitz, *On War,* ed. and trans. by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 92.
[13] Clausewitz, *On War*, 92.

scene with a gun," but that man may be a police officer instead of an infantryman if the enemy agrees to surrender the territory without a major battle. Wylie summed it up well when he said,

> As we have noted before, it may well be necessary to defeat the enemy army. It may even be necessary to defeat it to the last remnant. But if we always saddle ourselves with the self-imposed restriction that we must, no matter what, defeat the enemy army in combat, then we have indeed denied to ourselves consideration of a vast span of actions that might more readily and easily achieve the needed measure of control.[14]

Even if a combatant has won the battle or achieved a settlement, there may be a second step to achieve the "needed measure of control."

A signed peace treaty or a battle won may not be sufficient to establish meaningful control over territory if the population does not accept that control. If a combatant intends to establish land domain superiority in an area that previously belonged to the enemy, destroying or disrupting the enemy army, or forcing a settlement is often only the first step. Step one of destroying the enemy army gives a combatant physical access to the terrain where he can start step two of gaining population acceptance of that control. Lonsdale has highlighted the importance in land superiority of getting the "man on the scene with a gun" in place to start the struggle for the population. The criticality of the soldier or police officer is that only he can, "provide prolonged, durable presence and exert control over the key issue, whether that be a population or some other resource."[15] The recent wars in Iraq and Afghanistan have once again clarified that physical access to the terrain is only the precondition for the fight to gain

[14] Wylie, *Military Strategy*, 85.
[15] Lonsdale, *The Nature of War in the Information Age*, 211.

the acceptance of the population, and does not represent "mission accomplished." These concepts require some modification to the generic model of how to gain superiority.

In the land domain, there is not a clear difference between offensive and defensive forces as there is in the air or cyberspace domains. As a result, the universal forces under offensive and defensive collapse together, as they are generally the same forces whether a combatant assigns them offensive or defensive missions. The offensive and defensive split is still evident in local superiority as local forces are a smaller subset of the universal pool of forces that are not simultaneously attacking and defending in a local area. Losses at the local level feedback into the overall universal force whether the local force was on the defensive or offensive. One area where the land domain superiority model aligns with the generic model is in the equal weighting of local and universal superiority.

In the land domain, both the universal and local levels of superiority are important and receive equal weight in the model. This equivalence partially results because a combatant can use the same forces for offense and defense, which increases the importance of the universal level. However, strategic mobility can be slow in the land domain and it can take a long time to move ground forces from one local area to another, which increases the importance of the local level. In addition, land forces tend to be equally vulnerable at both the local and universal levels as a combatant can more easily disperse and hide forces than in the other domains. Also, a nation generally has far more tanks and artillery pieces than ships and aircraft so the loss of a few systems in the land domain normally does not have the same impact of losing the same number of ships or aircraft. The equal balance between the universal and local levels in the land domain is very unlike the cyberspace domain where the local level is dominant in cyberspace

superiority. The modified model of gaining and utilizing land domain superiority is in figure 4.

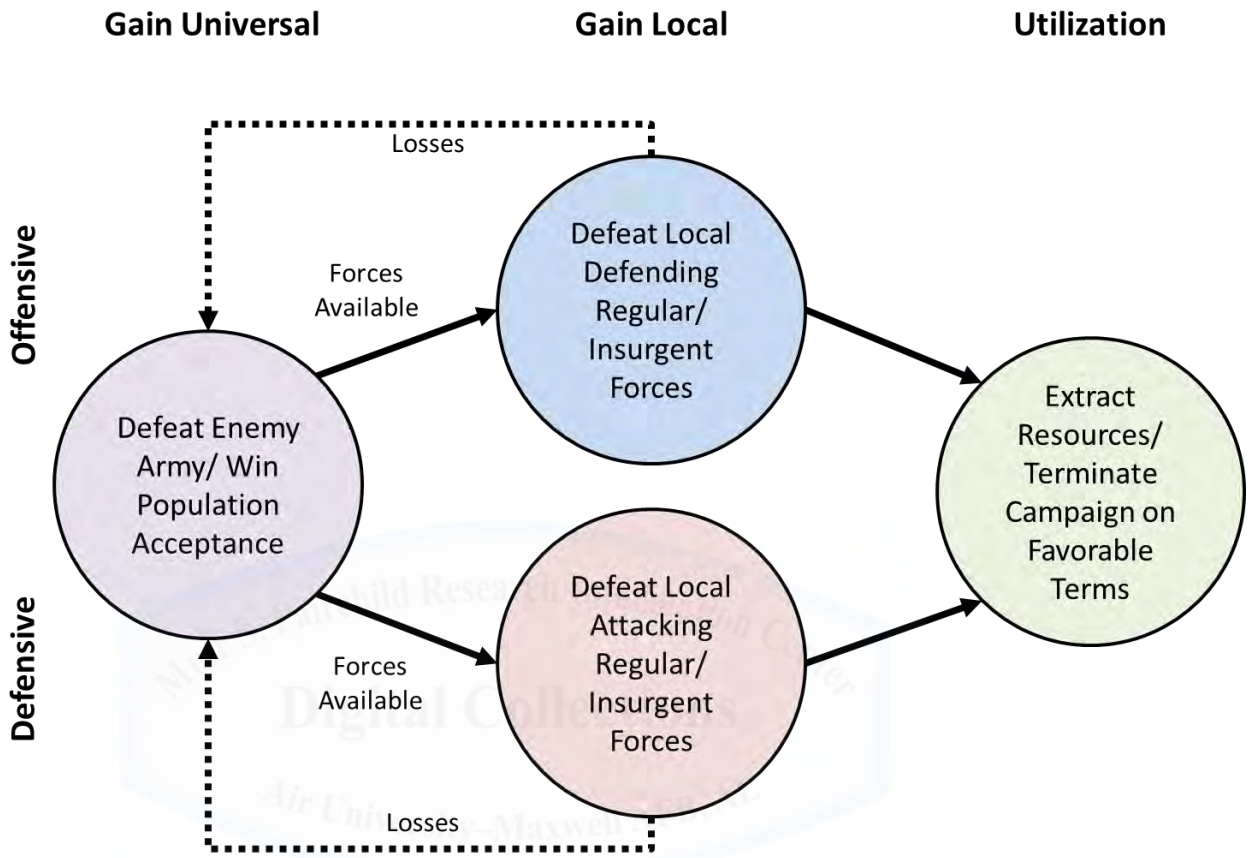

Figure 4 – Model of Gaining and Utilizing Land Superiority
Source: Author's Original Work

Gaining land superiority will be very different from gaining cyberspace superiority. Both the universal and local level of land superiority, defeat of conventional forces is a prerequisite for land superiority, but a combatant will not be able firmly to establish superiority or control over an area until the local population accepts it. There is no equivalent to population acceptance in cyberspace. In the land domain, both universal and local superiority are important, in the cyberspace domain, the local level is dominant.

When a combatant in the land domain has achieved defeat of enemy forces and the acquiescence of the population, he or she can exploit that victory.

Use of Land Domain Superiority

Once a combatant establishes superiority in the land domain to include the acceptance of the situation by the population, he can normally dictate terms to the enemy or, if the overall conflict continues in other theaters, a combatant can utilize the local area where the combatant has superiority to produce additional resources. These resources can include raw materials, finished goods or weapons, or even soldiers. A combatant can use the resources from the land domain to generate power in the other domains. Unlike the other domains such as maritime or air where control of the domain is principally of value as a way to influence the other domains, on the land, control is about affecting the enemy center of gravity. According to Wylie, the primary aim of the strategist is to exert some degree of control over the enemy, which a combatant normally achieves through manipulation of the center of gravity of the war to the advantage of the strategist.[16] Historically, this center of gravity has most often been control of territory or the resources that a combatant can extract from that territory. Land superiority provides both. Control of territory is important for both the attacking and defending sides, which causes the defensive and offensive sides of the generic model to collapse into a single circle for the utilization of land superiority.

A second change to the generic model of land superiority is that the utilization of superiority is the same whether a combatant is on the offensive or defensive. Both the

[16] Wylie, *Military Strategy*, 91.

attacker and defender are attempting to extract resources and control the terrain. The situation is quite different in the cyberspace domain where both sides are not trying to accomplish the same objectives in an attack. When a land force is contesting an area, such as the Germans and Soviets contesting for Ukraine in World War II, they both are normally seeking similar things. In the Ukraine case, both sides wanted the grain and other resources they could extract from Ukraine, and the opportunities for further offensives offered by the geographic position of Ukraine. In cyberspace, the attacker is normally trying to disrupt while the defender is trying to protect. However, nation A's success in attacking does not imply any success in defending; both combatants could be equally, or differently, successful or unsuccessful. Thus, in cyberspace, I separate the utilization of superiority into offensive and defensive aspects, unlike the land domain where I combined them in the model. That said, once a combatant has established land superiority, it will tend to be more persistent than is common in the other domains.

Persistence of Land Domain Superiority

Land domain superiority tends to be persistent due to greater influence of the universal level of superiority as well as the sequential tendencies of land combat, the inertia of populations whose support changes slowly, and the current primacy of the defensive.

The larger influence of the universal level of superiority in the land domain is the first factor producing greater persistence for land superiority. The combination of the ability of most land forces to perform both offensive and defensive missions, as well as to shift rapidly from one local area to another via modern transportation, normally means that combatants cannot just overcome a small subset of enemy forces to establish land

superiority in a local area. A combatant in the land domain who is attempting to wrest superiority in an area from the enemy must not only defeat the enemy defensive forces there before the attack, but also block the transfer of the reinforcements the enemy rushes to the scene who may have been performing offensive versus defensive missions elsewhere. This ability to reinforce is not common in the cyberspace domain. If an attacker in cyberspace overcomes the defenses on one system, the defender cannot simply move defenses from a different system, and cannot utilize offensive weapons as defenses on the system under attack. The importance of the universal level of superiority is one reason why the persistence of superiority in the land domain tends to be much longer than in the cyberspace domain.

The second factor is the sequential characteristic of land combat, which has generally tended to slow the pace of change of who has superiority in a given area. The geographic bounding of the land domain normally restricts changes in superiority to small areas. Taking a fortress only yields superiority in the area formerly controlled by that fortress and crossing one river opens up only the land area to the next geographic feature or defensive position. It is also difficult for a combatant who experiences a string of defeats to reverse the trend. The sequential characteristic of land combat does not only apply to geography, but also to time. The defeated side normally loses more resources than the winning side, although there are exceptions. Therefore, the side that was defeated last time is more likely to be defeated next time. The sequential characteristic of land combat contributes to the persistence of land superiority, which the inertia of populations further reinforces.

Populations link their political loyalty to language, culture, and identity and this loyalty is extremely difficult to change, which is the third factor increasing the persistence of land superiority. Conquerors are often surprised at how difficult it is to change substantially the loyalty of a population. For example, after 70 years of varying levels of ruthless subjugation, non-Russian Soviet states immediately reasserted their national identities and loyalties. Even after generations of heavy-handed attempts to eradicate their languages and change their cultures, the Soviets had still failed to subordinate their population's national consciousness and loyalties to the model of the Soviet "new man." As Americans, we of course thought we could do it much better and faster; and we attempted to remake Afghan tribal society and loyalties in a few years while failing just as spectacularly as previous invaders. Populations' resistance to change contributes to the persistence of long-term land superiority, and the advantage of the defense affects short-term land superiority.

The current primacy of the defensive is the final factor contributing to the persistence of land superiority, as two equally matched forces will be able to hold what they have, but will generally be unable to defeat successfully the other force. As I discussed previously in the section on offensive and defensive primacy, the fact that an advancing attacker is normally far more vulnerable than a hidden or entrenched defender creates the primacy of defense in the land domain with current tactics and technology. This factor also contributes to the greater persistence of land superiority as attacking forces will normally have to establish clear superiority before their attacks can be successful and even start the process of changing land superiority in a local area. If an analyst only considers the major wars in the last few decades, this superiority of the

defensive may not be immediately obvious as the defenders in Iraq and Afghanistan were quickly defeated. However, the United States had overwhelming superiority in technology, tactics, and even numbers in most battles; and these factors overcame the advantages of the defensive. Measuring how persistent land superiority is will require measuring land superiority in general, and I will next turn to this difficult problem.

Measurement Concepts of Land Domain Superiority

Land superiority consists of territorial control and population acceptance of that control; territorial control by itself is necessary but insufficient without population acceptance. Measuring whose soldiers are standing on a particular piece of terrain is by far the easier task and is how combatants have historically measured land superiority. According to James Clancy and Chuck Crossett, "In the grand movement of military forces, the gaining and control of territory is considered success."[17] From the Napoleonic wars to modern times, staff officers have drawn lines on maps that clearly delineated what areas friendly forces controlled and what areas were enemy controlled. The second part of the equation that planners generally examine is how many soldiers each side has available to occupy the terrain.

Since the universal level of superiority is so important in the land domain, another way to measure land superiority is to examine how many forces each side has on the universal level that a combatant can utilize to contest superiority at the local level. Clancy and Crossett refer to this traditional metric of success as the order of battle.[18] It is

[17] James Clancy and Chuck Crossett, "Measuring Effectiveness in Irregular Warfare," *Parameters*, Summer 2007, 90.
[18] Clancy and Crossett, "Measuring Effectiveness in Irregular Warfare," 90.

important of course not just to look at numbers and weapons but tactics and training as well in order to develop a comparison of combat power. A combatant should use both the measurement of terrain controlled as well as combat power expressed as an order of battle to develop a sense not only of the current state of land superiority, but also the potential for the future. An example of this principle happened in the early stages of the Korean War when United Nations forces gained dominant land control over the enemy after the Incheon landings. In this case, land superiority was not secure as the Chinese had a large and capable army on the border ready to intervene. Measurements of territory controlled and forces available are an appropriate way of measuring control during the first stage of the fight to control terrain, but planners need to use a significantly different approach to measure the level of population control.

The precise metrics used to determine population support will vary with the conflict, and Clancy and Crossett broadly categorize them as measures of sustainability, legitimacy, and stability.[19] The first area to focus on is the sustainability of the enemy force, which can include the supply of material such as weapons to the enemy. It is important that measurements focus on how much material is getting to the enemy, rather than the amount of material seized by friendly forces, which is far easier to measure. Sustainability metrics also look at the financial backing supporters provide to an insurgent enemy and how that support changes over time, as well as the estimated number of active enemy fighters and supporters. These are very difficult things to measure with accuracy, and analysts have to apply measures appropriate to each specific

[19] Clancy and Crossett, "Measuring Effectiveness in Irregular Warfare," 96.

situation very carefully. It is easy for a combatant focus too much on sustainability measurements, as the second area of legitimacy is much harder to measure.

The population determines the legitimacy of a government, which can be determined using measures of legitimacy and the effectiveness of those measures. Election results, surveys of the population, and measures of government efficiency and corruption can be helpful here. These metrics will be harder to assign numbers to, as legitimacy is primarily in the eyes of the local population. The United Nations may view a government as legitimate, but that will matter little to the population if that government is unable to provide basic services, or if it appears that a hostile outside power is actually in control. Government legitimacy is important, but without the final category of stability, measures of sustainability or legitimacy may not matter.

The final stability metric attempts to measure the level of security and ability to function of a local society. The security aspect is somewhat easier to measure as most insurgent attacks leave a clear signature that analysts can track over time. Unfortunately, merely counting attacks may not yield a complete picture. If there were 100 attacks last week and only 50 this week, does that represent progress? What if each attack was four times as deadly as the previous week's attacks? What if the reason there were fewer minor attacks is that the enemy is preparing for a major attack? Analysts will have to carefully comb reports for the relevant messy details and not get lulled into presenting simple metrics that look good on a PowerPoint chart. The ability of a society to function can be more difficult to measure and requires developing an understanding of the daily lives of the local people and what types of markets, institutions, and infrastructure they require. Analysts will need to combine both security and societal functioning metrics

with legitimacy and sustainability metrics to determine who has superiority in the land domain. However, both land domain measures have limited utility in the cyberspace domain.

Order of battle information and metrics on population support do not apply very well to the cyberspace domain. Forces in the cyberspace domain are much harder to compare, as they tend to be unique, as well as extremely difficult to find. In addition, as population support is not an important determinant of cyberspace superiority; sustainability, legitimacy, and security metrics have little applicability. Cyberspace can potentially help to measure population support for the land domain, but these measurement concepts will not apply to the cyberspace domain as readily as will those from the maritime and air domains. Next, we turn from the land domain to the maritime domain, which has very different characteristics.

Maritime Domain

Geography and Characteristics of the Maritime Domain

The maritime domain consists of a bounded maneuver space accessed by technology that is principally important due to the sea lines of communication that carry most of the world's cargo.

The air and land domains bound the maritime domain at its edges. This bounding produces an uneven, normally un-commanded domain with multiple strategic chokepoints as well as large open areas. This bounding is the first major characteristic of the maritime domain.

The maritime domain started out as a two-dimensional surface, bounded by landmasses, in the 20th Century expanded to a third dimension with the inclusion of undersea warfare. Technology is required to access the maritime domain much as is the case in the newer air, space, and cyberspace domains. The boundaries between the maritime domain and other domains define the edges of the domain.

The maritime domain, like the land domain, has distinct edges with the other domains; however, unlike land, the maritime domain produces its most significant effects in the other domains. The defeat and destruction of the Spanish Armada by a storm was most significant because it prevented Imperial Spain from conquering England on the land. The Battle for the Atlantic in World War II was important because it determined whether the United States could keep England supplied with vitally needed resources required by those living on the land. A nation can deter or compel its enemies by threats to enemy seaborne commerce as the Royal Navy effectively did for many years; however, maritime power has had its greatest impact in projecting power ashore. Since World War II, maritime power, in the form of aircraft carriers, has also been able to project significant power into the air domain. Maritime combatants have projected this power from an area that became the first recognized global common.

Modern international law considers significant portions of the maritime domain as a global common to which all nations have free access.[20] The United Nations Convention on the Law of the Sea (UNCLOS) considers the high seas far from land as a global common, as opposed to territorial waters and economic exclusion zones closer to

[20] Major General Mark Barrett, Dick Bedford, Elizabeth Skinner, and Eva Vergles. "Assured Access to the Global Commons." ed. by Supreme Allied Command Transformation. (Norfolk, VA: North Atlantic Treaty Organization, 2011), 5.

land. According to Article 87 of the UNCLOS, nations have freedom of navigation as well as other rights on the high seas.[21] This right of non-interference on the high seas is of critical importance to marine commerce, and now many policymakers are attempting to establish the same expectations and norms in cyberspace. However, the movement of information through cyberspace is not completely analogous to the movement of maritime shipping. Individual actors that reside within international borders own all the computing devices and network connections that create cyberspace, unlike the international high seas. Despite the differences in the domains, there is a significant effort underway in international circles to create the structures and norms to treat cyberspace as a global common. Despite lawyers labeling it a global common, the maritime domain still has numerous chokepoints that constrain maritime lines of communication.

The interaction of the land domain with the maritime domain produces a large number of chokepoints that become important strategic terrain in the maritime domain. These chokepoints funnel movement and are a key characteristic of the maritime domain, as those chokepoints become strategic areas for a combatant to control.[22] We will see a similar dynamic in the cyberspace domain where limited undersea cables or portals into a particular nation can become equivalent strategic chokepoints. The two most prominent theorists of the maritime domain, Mahan and Corbett, both focused their work on the importance of controlling lines of communication in the maritime environment. I will

[21] United Nations, *United Nations Convention on the Law of the Sea* 1994, 57. http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.
[22] McCarthy, "Traveling Domain Theory," 74-75.

weave their differing theories of maritime domain control throughout this section, but first I will discuss Corbett's idea that normally no one has maritime superiority.

Since the seas are so vast, and there are so few ships on them, Corbett maintained that normally no one has maritime superiority.[23] Admiral Gabriel Darrieus, a French Admiral writing in 1907, agreed with Corbett and thought it was "megalomania" to think that real "mastery of the sea" was even possible.[24] The concept that the sea is normally un-commanded by either side will translate well into the cyberspace domain, where private individuals normally own domain elements and domain architecture allows transit virtually at will. This open architecture results in a situation similar to the high seas, where the vast majority of traffic flows without any interference by either side of a conflict. The openness of the maritime domain also has significant impact on whether the offense or defense has superiority.

Offensive or Defensive Primacy in the Maritime Domain

In the maritime domain, neither the offensive or defensive has clear primacy; it depends on the specifics of the engagement. In most land combat, an approaching enemy has to "unmask" and come out into the open to attack. The defending soldiers can continue to hide under cover and can fire effectively on the advancing enemy, which provides much of the defensive advantage. In the maritime domain, however, surface ships are generally "unmasked" whether they are on the offensive or defensive so there is no clear advantage to being on the defensive. Lord Nelson believed in aggressive attack,

---

[23] Sir Julian Stafford Corbett, *Some Principles of Maritime Strategy, Classics of Sea Power,* (Annapolis, MD: Naval Institute Press, 1988), 91.
[24] Admiral Gabriel Darrieus, quoted in Beatrice Heuser, *The Evolution of Strategy: Thinking War from Antiquity to the Present* (Cambridge: Cambridge University Press, 2010), 244.

not because attacking made his ships relatively more powerful, but he thought that his better-trained and aggressive crews would win in the confused melee after breaking apart the enemy formation. At Jutland, the British fleet was on the strategic defensive and the German fleet was on the strategic offensive, but that meant little at the tactical level. Both fleets could see and fire on one another at roughly the same time, so being on the attack or defense gave no advantage one way or the other. There are other types of maritime combat other than fleet action where there is an advantage for the defense.

In undersea combat, the advantage goes to the one who stays hidden, which gives a benefit to the defense, as it is easier to stay silent and hidden. This situation is analogous to that of an infantry unit who can wait quietly in hidden positions until the enemy advances and becomes vulnerable. Another type of maritime combat that gives an advantage to the defender occurs when the defender can call upon land-based combat power and defenses.

A fleet operating within range of friendly land based defenses gains a significant advantage. This factor has normally helped the fleet defending its home territory although with aircraft it is possible that both the attacking and defending fleets will be within range of each other's airfields. Some of the naval conflict in the English Channel between Germany and Britain during the early stages of World War II illustrates a case where both sides could send land-based aircraft into a disputed maritime area. Historically, the more common situation has been where a defensive fleet sheltered behind minefields, coastal guns, or aircraft in a port. The French fleet in the Napoleonic wars and the German fleet in World War I are two of the most famous examples. A fleet in such a defended position can be very difficult to attack although there are cases such as

Taranto and Pearl Harbor where attackers accomplished it successfully using the element of surprise. The case of a fleet in port has interesting parallels in the cyberspace domain.

Cyberspace "fleets" shelter behind cyberspace defenses that cannot take part in offensive operations akin to a maritime fleet defended by port defenses. Mahan saw maritime defenses such as coastal guns as protecting and providing a secure base for the maritime offense in the form of the fleet.[25] Cyberspace defenses serve to protect the systems used to develop and field offensive weapons. Cyberspace defenses also protect the "ports" where commerce flows, but the analogy breaks down when it comes to how a combatant gains maritime versus cyberspace superiority. Maritime weapons such as ships can generally engage each other out on the high seas wherever they meet; cyberspace weapons cannot, which makes the gaining of maritime superiority very different from cyberspace superiority.

Method of Gaining Maritime Superiority

Theorists have disagreed on the relative importance of the local or universal level in gaining maritime superiority. For Mahan, the only way to gain maritime superiority was to destroy the enemy's fleet, while Corbett saw other possibilities. According to McCarthy, the central idea of Mahan's thesis was that ensuring access to maritime lines of communication was only possible through the neutralization of the enemy's fleet by your own fleet action.[26]

[25] Alfred T. Mahan, *Mahan on Naval Strategy: Selections from the Writings of Rear Admiral Alfred Thayer Mahan*, Edited by Allan Westcott (Boston: Little, Brown, and Company, 1918) 129.
[26] McCarthy, "Traveling Domain Theory," 81.

Corbett had a more complex view and saw additional possibilities. He believed that a combatant could achieve maritime superiority by either destroying the enemy's fleet or by blockading it in port. Corbett also thought that a navy could contest the command of the sea by maintaining a fleet in active service that only gave battle on favorable terms and launched small counter-attacks whenever possible.[27] He thought this strategy was possible because a fleet was nearly impossible to destroy in a well-defended harbor absent a land invasion to seize the port. As we examine Mahan and Corbett's ideas in relation to cyberspace, Corbett's ideas seem more pertinent to this project.

Corbett's methodology for gaining maritime superiority has more applicability to cyberspace superiority than Mahan's concept, as cyberspace "fleets" cannot meet and do battle. Offensive cyberspace weapons are as difficult to attack "in port" as a well-defended fleet, and simple force on force battle is impractical in cyberspace, as the weapons cannot normally sense and react to each other, as can ships at sea. As a result, cyberspace weapons will go right past each other if they cross in cyberspace, more like cruise missiles en route to targets than ships or fighter aircraft that can fight each other when they meet. This difference between cyberspace and the other domains will be crucial to understanding how to gain superiority in the cyberspace domain. To understand further gaining maritime superiority, it is helpful to break it down into its universal and local components.

In the maritime domain, combatants can more easily contest superiority at the universal level by attacking the enemy's fleet than in the other domains. Destroying the

[27] Corbett, *Some Principles of Maritime* Strategy, 165.

enemy's fleet will significantly affect the resources available to contest superiority at the local level, but normally only if the enemy is willing to cooperate and fight a major fleet battle. Mahan's theory focuses on a major fleet battle and if the enemy fleet is willing to sail out and be defeated, then the winning combatant can disperse his victorious fleet to attack enemy shipping and defend friendly shipping with confidence. What Corbett saw is that the weaker party will often not be willing to sail out to be defeated. Instead, the weaker force can avoid major battle but remain as a threatening "fleet in being" that can retreat to a fortified port if pressed too closely. This action puts the stronger combatant on the horns of a dilemma because if he disperses to attack and defend commerce, the enemy can sally forth and defeat elements of his fleet before he can concentrate. A weaker combatant can avoid a universal fleet battle and instead fight a small series of local actions.

A combatant can send out cruisers to attack enemy shipping while avoiding the enemy's stronger battle fleet. This strategy can rob the stronger navy of most of his ability to control the sea lanes and project power because his fleet has to remain constantly ready to fight the weaker navy. Mahan focused on the destruction of the enemy fleet and expected that "command of the sea" would go to the victor of the fleet battle. However, the experience of World War I showed the importance of Corbett's "fleet in being" concept as the mere presence of the German fleet in port forced the British to keep their fleet concentrated in case the German fleet sailed out. In the one case where the German fleet did sail forth, the ensuing battle proved indecisive. However, since the British fleet was still concentrated, it could not focus all its resources on protecting the sea lines of communication under attack by German U-boats, which in

this case took the place of Corbett's "cruisers." Despite the utility of a weaker combatant contesting superiority at the local level, the universal level of maritime superiority carries more weight.

In determining superiority in the maritime domain, the universal level is of greater importance than the local level due to a number of factors. First, maritime forces can normally perform offensive or defensive missions, which allow a combatant to use universal forces either way. A destroyer, submarine, or even carrier battle group can attack enemy targets or defend friendly ones with a similar level of efficacy. Second, maritime forces tend to have better strategic mobility than the land or air domains, and can move from one local area to another with greater speed and over longer distances than land forces, while not needing the elaborate, and slow to build, airfields of the air domain. Third, ships are expensive and nations tend only to have a few of them so they represent a more concentrated form of national power than is typical in the land or even air domain. Therefore, destroying or degrading even a handful of ships will more greatly affect the forces a combatant has available to contest local superiority in other areas. All these factors, combined with the vulnerability of maritime forces at the universal level to attack, contribute to the relatively greater level of importance for universal versus local maritime superiority. The modified model of gaining and utilizing maritime superiority is in figure 5.

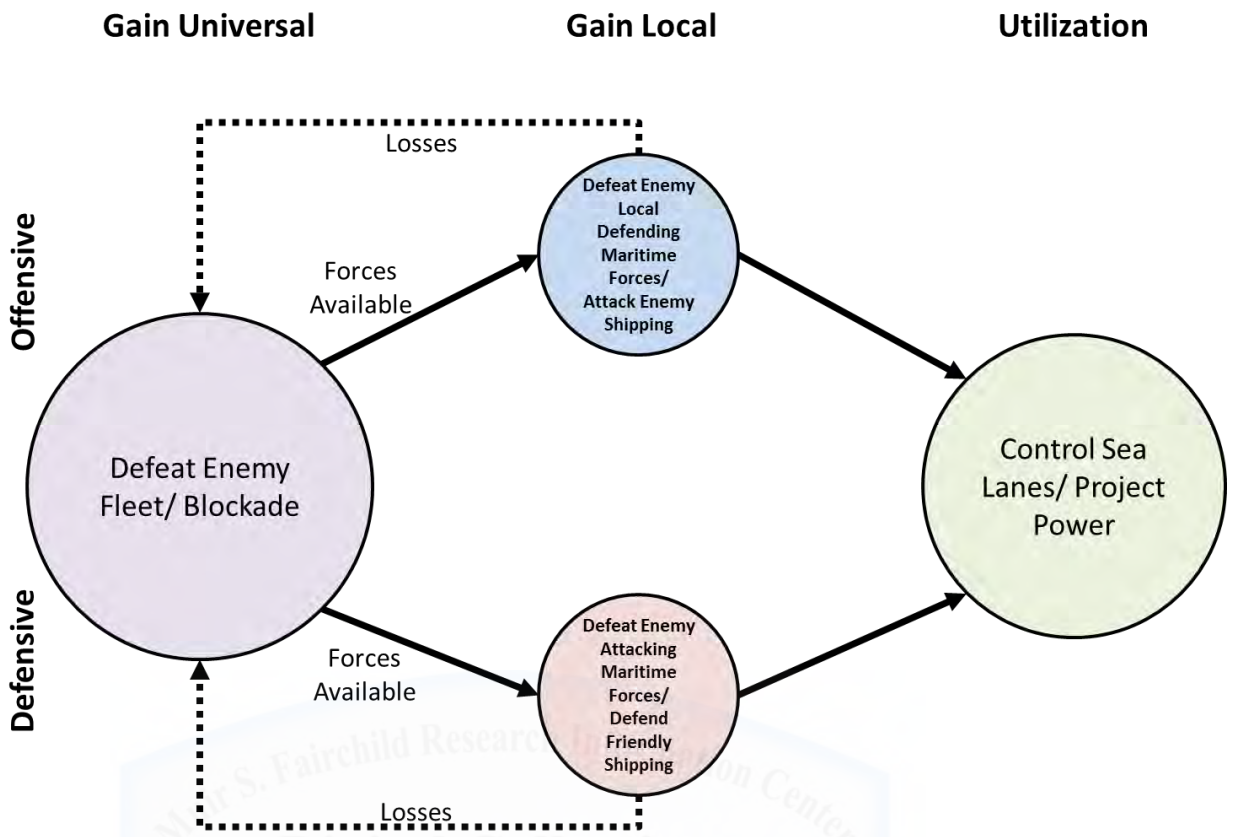

Figure 5 – Model of Gaining and Utilizing Maritime Superiority
Source: Author's Original Work

Although the universal level is more significant, it is still possible for a combatant to achieve maritime superiority by focusing on the local level. If defeating the enemy fleet is not an option, there is also a longer and harder road of attritional "war of a thousand cuts." Eventually this strategy can produce a level of universal maritime superiority as the resources available to the enemy continue to shrink if the losses from combat at the local level accumulate faster than the enemy can acquire more forces. Mahan was dismissive of commerce, or local warfare.[28]

[28] McCarthy, "Traveling Domain Theory," 81.

Corbett, on the other hand, thought a combatant could exercise domain control by using cruisers optimized to seize enemy shipping while avoiding the enemy's main battle fleet and saw utility in blockades. Corbett also proposed a different way for a combatant to attain some level of universal superiority through blockading the enemy's fleet in port. If a combatant successfully blockades the enemy fleet, then at least some of his lighter units can engage in attacking enemy commerce and protecting friendly shipping. While Corbett's commerce warfare has parallels in cyberspace, his "fleet in being" as well as Mahan's fleet battles and blockades do not have direct equivalents in cyberspace.

Much of the current combat in cyberspace looks analogous to Corbett's commerce warfare. In Corbett's commerce warfare, attackers would attempt to interfere directly with an enemy's commercial maritime activity, while defenders would attempt to protect their commerce. In cyberspace, most current conflict involves disruption of commerce, theft of information, or attempts by defenders to prevent successful attacks. Just as the principal utility of the maritime domain is moving goods, the principal utility of the cyberspace domain is moving information, which sets up some similar dynamics. One of Corbett's concepts with less applicability to cyberspace is the fleet in being.

Although cyberspace forces are very difficult to attack "in port," they cannot act as a fleet in being, as they cannot force the enemy to divert resources in order to prevent them from sallying forth. In the maritime domain, a fleet in being principally acts to keep the enemy force concentrated so that it cannot engage in commerce warfare. Since neither combatant can easily attack the other's cyberspace "fleet," there is no need for forces to remain concentrated and both sides can engage freely in cyberspace warfare in various local areas. Cyberspace forces can potentially act as a deterrent since combatants

cannot easily attack them; however, they are no different from any other domain force. What cyberspace forces cannot do is force the enemy to divert resources and remain concentrated to fight a fleet action if the fleet in being sorties out. Combatants also cannot easily blockade cyberspace forces.

The inability of combatants to directly attack or block enemy cyberspace forces also prevents the maritime concept of a blockade from transferring to cyberspace. Cyberspace weapons are stealthy and a combatant can launch them from almost anywhere so it is extremely difficult to "blockade" them. Even severing an enemy nation's connections to the Internet would not be a sure defense as enemy agents could still easily insert weapons from other locations. In maritime surface warfare and cyberspace, there are some parallels with commerce warfare; however, there are better parallels to cyberspace in undersea warfare.

The situation in cyberspace is analogous to a struggle for maritime superiority undertaken by fleets composed entirely of super-stealthy submarines. One of Mahan's key assumptions was that each fleet could effectively find and attack the other. If each combatant had a fleet consisting of only super-stealthy submarines then they could not effectively find or attack each other's combat forces, but only attack surface shipping. Then, attacking the enemy fleet or conducting a blockade becomes meaningless and there is no conceivable fleet action to deliver maritime superiority. Both combatants would have to mitigate the damage caused by enemy submarines while attempting to maximize the damage done by their own.

This circumstance parallels the situation in cyberspace where cyberspace offensive weapons cannot find or engage each other. Some attempts to reduce the

enemy's offensive capability such as attacking submarine pens in the maritime realm or bombing a cyberspace operation center may be worthwhile, but effective opportunities to do much damage will be rare. The next question after successfully gaining maritime superiority is what to do with it.

Use of Maritime Superiority

Once a combatant gains maritime superiority, he or she can protect friendly sea lines of communication and attack those of the enemy, while enabling friendly power projection ashore and preventing enemy power projection. Corbett identified the same categories although he broke it up slightly differently into defense against invasion; attack and defense of commerce; and attack, defense, and support of military expeditions.[29] Maritime superiority enables a combatant to control the sea-lanes, which enables friendly shipping while interfering with enemy shipping.[30] Maritime superiority also affects enemy power projection, which Corbett identified as defense against invasion. Power projection ashore is a critical element of maritime superiority.

While Mahan viewed sea power as critical to a nation in its own right, Corbett saw the greater importance in the maritime domain as lying in what it could do to influence the land domain.[31] For Corbett, the reason why sea lines of communication were so vital is that they enabled the projection of power ashore. Superiority at sea principally mattered because it could provide superiority on the land. Cyberspace is similar to the maritime domain in this respect.

---

[29] Corbett, *Some Principles of Maritime* Strategy, 165.
[30] Alfred T. Mahan, *The Influence of Sea Power Upon History, 1660-1783* (New York, NY: Dover Publications, 1987), 26. and Corbett, *Some Principles of Maritime* Strategy, 93.
[31] Corbett, *Some Principles of Maritime* Strategy, 16.

A combatant will feel the most important effects of cyberspace superiority, not in cyberspace, but in the other domains. Disrupting enemy communications matters most if a combatant can use that disruption to attack in the other domains. Defending friendly systems enhances the ability of a combatant to generate and utilize power to establish superiority in the other domains. As an example, consider the cyberspace systems that support a Combined Air Operations Center (CAOC). The most important effect of disrupting those systems may not be in the cyberspace domain, or even in the air domain. If an enemy disrupted command and control systems in the middle of a major land offensive, the loss of the cyberspace systems could result in the reduction of coordinated close air support over the battle and lead to the loss of the battle in the land domain. All the domains have connections, but cyberspace is the most interconnected and combatants have embedded cyberspace in all the other domains through modern information systems. Turning back to maritime superiority, the next question is how persistent maritime superiority will be once a combatant has attained it.

Persistence of Maritime Domain Superiority

Whether the maritime superiority gained by a combatant is local or universal will greatly affect the persistence of maritime superiority. If a combatant gains only local superiority, then the enemy can transfer forces from the universal level by moving them into the local area and fight for superiority again. If a combatant gains a significant level of superiority on the universal level, the enemy has to create, purchase, or get new forces from allies, which will normally take much longer than merely moving forces from one area to another. This ability to reinforce from other areas is especially true in the maritime domain where strategic mobility is usually very good. However, just because a

combatant loses overall universal domain superiority, it does not follow that he will lose local superiority in every local area. The losing combatant may concentrate his remaining forces in a different area than his adversary and still attain superiority in that local area. In the maritime domain, Mahan and Corbett disagreed on whether maritime superiority tended to be persistent or not, largely because they differed on how universal or local it was.

According to Mahan, who focused on universal maritime superiority, superiority should be persistent based on major fleet actions that would affect universal superiority. Much like the battle of armies on the land, if a combatant fights and wins a major fleet action it will provide some measure of persistent superiority, as it is hard for the enemy to win the next battle with diminished resources. Corbett questioned Mahan's idea of stable overall command of the seas and asked about an enemy who chooses not to fight a fleet action.

If the enemy refuses to fight a major fleet action for universal control, then control will not only be localized, but also fleeting as the enemy can dash out of port to raid convoys and establish local control in an area, and then retreat back into port when threatened by the main adversary fleet. The French fleet used this strategy during much of the Napoleonic wars. The British attempted to blockade the French fleet in port, but they could not stop a steady stream of French cruisers from slipping through the blockade to raid British merchant shipping, as the French established local maritime superiority in their operating areas. Also, the British had not established universal superiority as the French fleet was still formidable, and the French could contest local superiority in the area of the blockade at any time by sailing out. The British were unable to establish

stable maritime superiority until they had largely destroyed the French fleet at Trafalgar. Unfortunately for cyberspace operators, the inability for cyberspace forces to fight the equivalent of a fleet battle suggests that the persistence of superiority will be limited in the cyberspace domain.

Since cyberspace forces cannot engage each other in fleet actions and normally have to contest superiority at only the local level, the linkage in the maritime domain between persistence and universal superiority suggests that cyberspace superiority will have a short duration. The speeds at which combatants can develop weapons in the maritime and cyberspace domains also suggest short duration for cyberspace superiority. In the maritime domain, where producing a major combatant takes years, domain superiority can be persistent if universal superiority is gained by a combatant. In the cyberspace domain, on the other hand, even if a combatant achieves a high level of domain superiority, the enemy could develop, or purchase from an ally, an entirely new set of weapons or defenses in weeks or months. This difference between the maritime and cyberspace domains further suggests that cyberspace superiority will be fleeting. The final area of maritime superiority to examine is how analysts have measured it over time to determine if there are elements of measurement that may be applicable to cyberspace.

Measurement Concepts of Maritime Superiority

Traditional measures of maritime superiority include the balance of forces between the two fleets, metrics to measure the openness of sea lines of communication, and the ability of combatants to project power from the maritime environment into other

domains.[32] The balance of forces can include the total number of ships, the type of ships, and tonnage or the combined weight of ships. Analysts should use these numbers with care, as the material aspects of a navy are only part of the story. During the Napoleonic wars, the British routinely outfought opponents who had heavier, faster, and better armed ships because the British had better morale and much better training. As noted earlier, the balance of forces is only theoretical until a combatant induces the enemy to come out and fight.

The balance of forces will only produce equivalent maritime superiority if combatants are both fully utilizing their forces. If one fleet stays in port, the one out on the high seas will have the greater measure of maritime superiority in that local area. That local superiority may be transitory and persist only until the enemy fleet comes out of port to contest it. Mahan focused his measurement of maritime superiority on the balance of forces between the two fleets. If the combatant had fought and won the fleet battle, then he had established maritime superiority, although Mahan did recognize maritime superiority did not imply that enemy ships could not operate at all.[33] Comparing maritime forces is only part of measuring maritime superiority; analysts must also consider the health of sea lines of communication.

There are numerous ways to measure the health of sea lines of communication to include percentages of friendly shipping that make it safely into port, the tonnage of enemy shipping seized, etc. There are two parts to the analysis of sea lines of communication; are friendly forces able to ship material, and is the enemy able to ship

[32] Clancy and Crossett, "Measuring Effectiveness in Irregular Warfare," 90.
[33] Mahan, *Influence of Sea Power Upon* History, 14.

material. They are both elements of a related question of who is able to use the maritime domain effectively. An analyst needs to make sure that he or she examines both sides and much like in the land domain, the analyst will need to choose the metrics with care. For example, the amount of enemy tonnage getting to the enemy will likely be more important than the amount of tonnage that a combatant has sunk although it is harder to measure. A final area of measurement in the maritime domain is power projection from the domain.

If combatants can project power from the maritime domain into other domains, it implies a significant level of maritime superiority. Amphibious landings or raids and projecting power into the air or space domains all imply a level of maritime superiority that analysts can observe and measure. Potential power in the maritime domain can affect the other domains even if a combatant does not choose to utilize it. One example of this principle in action was during the first Gulf War where the Iraqis dedicated a significant amount of resources to defend against an amphibious assault that the United States never launched. Some of these same types of measurements will also be useful in the cyberspace domain.

Comparing the balance of forces in the cyberspace domain is more problematic than in the maritime domain; however measuring the health of lines of communications and power projection into other domains has utility for the cyberspace domain. In the cyberspace domain, it is much harder to compare forces than in the maritime domain. Battleships and cruisers are much easier to compare than cyberspace weapons which are easier to hide and more difficult to compare. Measurement of the openness of cyberspace lines of communication is a more promising approach from the maritime domain. Also

measuring how well a combatant can project power from cyberspace into the other domains is a method that will have utility in cyberspace as well as the maritime domain. There are a number of concepts useful for cyberspace superiority that we can pull out of the maritime domain; the same is also true of the air domain where we turn next.

Air Domain

Geography and Characteristics of the Air Domain

The geography of the air domain is very different from that of land or sea and gives the domain its unique characteristics, including the fact that the air domain is mostly open and less constrained. While the air domain has boundaries below on the surface, and above in the limits of the atmosphere, there are no natural chokepoints such as mountain ranges and swamps, or reefs and straits in the horizontal dimension. According to McCarthy, "The air domain is free of geographic boundaries that define chokepoints and lines of communications on the land and within the maritime commons."[34] Early airpower theorist Giulio Douhet put it even more strongly when he said that the airplane had complete freedom of action and could fly anywhere without the possibility of interference by surface forces.[35] Douhet overstated the case and while there are not natural constraints, there can be man-made ones.

The air domain is not completely unconstrained; there can be man-made constraints in the air domain such as effective Surface to Air Missiles (SAMs). Ground based defenses set up by a combatant can form artificial chokepoints that are roughly

[34] McCarthy, "Traveling Domain Theory," 114.
[35] Giulio Douhet, *The Command of the Air* (1921; new imprint, Mechanicsburg, PA: Stackpole Books, 1999), 283.

analogous to land or maritime chokepoints. One major difference is that these chokepoints are very mutable and can be destroyed or moved much more easily than a mountain range or strait. The cyberspace domain has even greater tendencies towards mutability, as the entire cyberspace domain is artificial and constructed, where in the air domain, only the ground-based defenses move or change quickly. The open terrain of the air domain allowed air forces to bypass most defenses and attack deep into enemy territory.

A characteristic of airpower that is different from the land and maritime domains is that air domain forces can more easily bypass defenses to target directly civilians and infrastructure. According to Douhet, the battlefield would not be limited to only soldiers but all citizens would become combatants.[36] The German Zeppelin raids over London of World War I represented the start of this trend and presaged the wholesale destruction of German and Japanese cities using nuclear and conventional bombs during World War II. The cyberspace domain is similar to the air domain in this respect, as cyberspace attacks can bypass fielded military forces to affect directly civilian life and infrastructure, whether by design or as collateral damage. Both strategic cyberspace attacks on infrastructure, and attacks that get out "in the wild" and do things their designers did not intend exhibit this ability to affect directly civilians. Douhet identified that airpower had independence of surface limitations allowing direct attack on civilians, and also had the next key characteristic of speed.[37]

[36] Douhet, *The Command of the Air*, 283.
[37] Douhet, *The Command of the Air*, 289.

Another characteristic of the air domain is great speed of action compared to the land and maritime domains. This great speed results from the physical characteristics of modern aircraft that can move from place to place much faster than land or maritime forces. A second component to the speed of action of air domain forces is their ability to move unpredictably. Space vehicles, such as satellites, are far faster than aircraft in terms of velocity, but they are greatly constrained by the laws of orbital mechanics and so are also very predictable. Aircraft can easily feint in one direction before attacking in another. Clausewitz stated that the two basic principles underlying strategic planning were concentration and speed.[38] Airpower provides great speed, as well as the ability to concentrate rapidly.

The great speed, long range, and flexibility of modern aircraft make it very easy for air domain forces to concentrate rapidly on a mission or location. The multi-role capabilities of many modern aircraft contribute greatly to this characteristic. A multi-role fighter could launch from Al Udeid airbase in Qatar on Monday to do intelligence and surveillance in Iraq, fly close air support in Afghanistan on Tuesday for ground forces, and then provide a defensive combat air patrol over shipping in the Persian Gulf on Wednesday. Land and surface forces generally take much longer to re-orient to different missions or to move physically to the area where they need to execute the new mission. Cyberspace shares many of these characteristics with the air domain.

Cyberspace is more like the air domain than the land and maritime domains in its speed of action and flexibility. While specific cyberspace weapons tend to be very

[38] Clausewitz, *On War*, 617.

tailored and unique to a single mission, the units performing those missions are not, and can rapidly shift from one mission set to another. The weapons of cyberspace can move even faster than aircraft and they often arrive at their destination in microseconds. Thus, cyberspace can also achieve great speed of action. Air domain forces rely on technology for speed of action, and for access to the domain.

Combatants access the air domain through technology much as combatants access the maritime, space, and cyberspace domains. Douhet identified that war in the air domain was heavily dependent upon the technical means available and would change rapidly over time. Douhet stated that, "The form of any war—and it is the form which is of primary interest to men of war—depends upon the technical means of war available."[39] In World War I, the rapidly changing technology had a major impact on who had air superiority. When the Germans had interruption gear that let them fire through their propeller arcs, but the French and British did not, the Germans had air superiority.[40] Once the French and British copied the technology, the fight was nearly equal, at least until the next technological innovation as the combatants were improving their aircraft at rapid rate. The pace of innovation in World War II was slower than World War I because the technology was more mature, but a similar dynamic was at work as technological innovation had a significant impact on who had air superiority.

---

[39] Douhet, *The Command of the Air*, 279.

[40] In 1915, a Frenchman, Roland Garros developed deflectors that enabled him to fire a forward facing machine gun through the propeller arc of his aircraft to deflect the 10% of bullets that would have hit the propeller. The system enabled him to shoot down three German aircraft before it disabled his aircraft and forced him to land behind German lines. When the Germans turned over the deflector to a Dutch engineer, Anthony Fokker, he developed a more sophisticated device that prevented the gun from firing when the propeller was in front of the machine gun. This technological innovation led to a period of German dominance of the skies over Europe called the "Fokker Scourge" until the French and British developed their own interruption gear about six months later. John H. Morrow Jr. *The Great War in the Air: Military Aviation from 1909 to 1921* (Washington: Smithsonian Institute Press, 1993), 92.

Despite the importance of technology in the air domain, technological advantage is not sufficient to determine air superiority. The Iran-Iraq war is one case where a lower technology combatant was still able to achieve air superiority despite technological disadvantages. Larger numbers, training, and tactics can all offset a combatant's superior technology. The technological edge of U.S. Air Force in North Vietnam was often offset by the better North Vietnamese tactics and training. The United States lost a number of expensive and high technology F-4s to lower technology MiG-17s and MiG-19s.[41] That these losses were driven by tactics and training versus technological shortcomings is illustrated by the very different levels of success achieved by the U.S. Navy and U.S. Air Force who were flying the exact same aircraft against the same enemy with different training and tactics.[42]

Technology is also tremendously important in the cyberspace domain, because combatants create cyberspace via technology. It is harder for cyberspace combatants to offset deficiencies in technology with tactics and training as there is less real time human interaction in cyberspace than in the air domain. One area where the air and cyberspace domains are quite different is in the cost of technological access to the domain.

Access to the air domain is expensive and requires both costly high technology aircraft and infrastructure in the form of airfields. Modern aircraft of all classes from fighters to transports are very expensive and involve long design and production lead times. The technology required for a functional airfield is not as advanced, but airbases

[41] For a detailed discussion of how poor tactics and training by the U.S. Air Force gave the North Vietnamese the edge in air combat see Marshall L. Mitchell III, *Clashes: Air Combat over North Vietnam 1965-1972* (Annapolis, MD: Naval Institute Press, 1997)
[42] Mitchell, *Clashes: Air Combat over North Vietnam 1965-197*, 4.

are massively costly infrastructure projects that normally take many years to plan and build. The United States has been fortunate to fight recent wars in areas where abundant oil money has built numerous large modern bases. Trying to carve a functioning fighter base and transport hub out of a remote location in sub-Saharan Africa would be much more challenging.

Fortunately for cyberspace operators, they do not require extensive infrastructure. In the cyberspace domain, the cost of entry is much lower and a cheap laptop and network connection may be all that is required to deliver a weapon, although developing the weapon will take more resources. The final characteristic of the air domain is one that the cyberspace and air domains share: success in the domain is neither necessary nor sufficient for attainment of military objectives.

The last characteristic of air superiority applicable to cyberspace superiority is that its importance is highly contentious. Some airmen have unfortunately felt the need to claim that airpower was all that a nation needed for success in warfare due to the long and bruising fights for organizational independence.[43] When these overenthusiastic predictions turned out not to be true, and the Germans did not surrender after the Allies destroyed German cities, analysts sometimes shifted to the other extreme of claiming that airpower accomplished nothing of significance. Both sides are wrong, air superiority is an important factor in modern warfare, but does not guarantee victory.

Air superiority is normally not sufficient to produce a successful outcome for a combatant by itself. However, it can certainly help a nation win a conflict. The wars in

[43] Gray, *Modern Strategy*, 228.

Korea and Vietnam, among many others, have shown that air superiority alone is not enough to guarantee victory. At the same time, no sane army officer would want to fight a war without air superiority if it were at all possible. Air superiority provides tremendous advantages to the side that has it. The never-ending debates over whether airpower or land power was "decisive" in the Gulf War provide little more than organizational cheerleading, not good analysis. The same dynamics that have produced contention about the importance of air superiority also exist in cyberspace.

Cyberspace superiority is even less likely than air superiority to prove necessary *and* sufficient to win wars despite its great potential to help achieve objectives. Cyberspace is a new domain whose support is immensely important to operators in the other domains. At the same time, cyberspace operators often feel that leaders downplay their ability to provide direct action through cyberspace to ensure that they stay organizationally under the thumb of officers who are from the other domains. Cyberspace superiority has an important role to play in both its own domain, and in supporting the other domains. In this way, it is similar to air superiority. Another area where there is some similarity between the air and cyberspace domains is that the technology of cyberspace drives the advantage for the offense or defense.

Offensive or Defensive Primacy in the Air Domain

While earlier air domain theorists favored the offensive, whether the defensive or offensive have primacy in the air domain has shifted over time with technological change. Douhet stated that the airplane was inherently offensive and completely unsuited

for the defensive based upon World War I air combat.[44] Colonel Billy Mitchell, who had far more experience in actual combat in World War I understood that aircraft could mount a successful defense through air combat.[45] In the interwar period, airpower theorists generally agreed with Douhet that the offensive had a significant advantage; Lord Stanley Baldwin famously stated that, "the bomber will always get through."[46] This theory was reasonable given the facts of the time, but it did not turn out to be correct.[47]

Several technological changes during and after World War II shifted air domain effectiveness to the defense. Fighter aircraft became more capable, radar allowed for early warning, and improved command and control schemes enhanced the effectiveness of the defense. Overwhelming numbers of aircraft on the side of the Allies proved decisive in the battle for air superiority in the European theater.

After World War II, the development of effective Surface to Air Missiles (SAMs) gave an entirely new category of tools to the defense that shifted the balance further towards the defense. Stealth technologies provided new avenues for the offense, which defenders have partially countered with new types of detection systems and improved

[44] Douhet, *The Command of the Air*, 355.
[45] William Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power, Economic and Military* (1925; new imprint, Mechanicsburg, PA: Stackpole Books, 1999), 502.
[46] Stanley Baldwin, "A Fear for the Future," Speech given in Parliament 10 November 1932. http://en.wikisource.org/wiki/A_Fear_For_The_Future.
[47] Analysts based the idea that bombers would always get through to their targets on several factors. One was that pursuit aircraft only had a slight speed advantage over bomber aircraft and took so long to get to altitude that the bombers would be gone before pursuit aircraft could engage them. A second was that bomber aircraft would be able to defend themselves with their own defensive firepower. Both concepts turned out to be wrong. Fighter aircraft developed a significant speed advantage over contemporary bomber aircraft, and radar as well as better command and control greatly enhanced their capability to intercept bombers and get to altitude before the bombers arrived. The bombers were much less able to defend themselves than expected because defensive gunners turned out to be less effective than analysts had predicted.

SAMs. These changes have brought the offense and defense in the air domain into rough balance.

Right now, there is no clear primacy to the offense or defense; the more effective operational and tactical force is likely to defeat its foe on either the offense or defense. The various conflicts fought by Israel demonstrate that the more effective Israeli Air Force was able to defeat its foes both when Israel started on the defensive in the Yom Kippur War, and on the offensive in the Six Day War and Bekaa Valley campaign. According to McCarthy,

> Today, with the benefit of extensive airpower history and an understanding of the maturity of air defense weapons, we know that air domain power is not inherently offensive in nature. Air defense assets can deny an enemy access to vital points and can wear down an attacking force, effectively eliminating an adversary's airpower through defensive action.[48]

A healthy understanding of the importance of both the offensive and defensive sides of combat in the air domain is critical to a proper understanding of how to gain superiority in the air domain.

Method of Gaining Air Superiority

Early airpower theorists focused on universal air superiority but they thought combatants could achieve it in different ways. For Douhet, the most efficient way of achieving air superiority was to attack the enemy aircraft on the ground.[49] Airpower theorist Alexander De Seversky agreed with Douhet that a combatant would win air superiority by attacking offensively, however Seversky focused on shattering enemy

[48] McCarthy, "Traveling Domain Theory," 185.
[49] Douhet, *The Command of the Air*, 307.

industry and not just attacking airfields.[50] Mitchell thought that the best way to destroy the enemy air force was to fight them in the air after forcing them up to fight by bombing targets the enemy would have to defend.[51] RAF officer and airpower theorist J. C. Slessor agreed with Mitchell, but put more emphasis on forcing the enemy to defend his vital centers while also attacking the enemy air force directly.[52] The common thread through all of these airpower theorists was offensive attack, either at the enemy air force directly, or at the industry and infrastructure that created and supported it. This correlates closely to land and maritime superiority concepts that involve defeating the enemy army or fleet respectively. A common concept with all these theorists is the idea that to gain universal air superiority, a combatant needs to attack enemy universal air domain forces.

As the earlier theorists identified, to gain air superiority at the universal level a combatant needs to attack the enemy's offensive and defensive air domain forces. On the offensive side a combatant should degrade the enemy strategic Integrated Air Defenses (IADS) as much as possible. These are the forces with a long enough reach to see and target attacking air domain platforms. Attacking the enemy strategic IADS has normally been the first step in any offensive air campaign as it enables the follow on portions of the campaign. On the universal defensive side, a combatant should degrade the enemy's offensive airpower as much as possible whether that is through strikes on airfields, missile launching and storage facilities, or other infrastructure. These are the first two elements of the model of gaining and utilizing air superiority in figure 6.

---

[50] Alexander P. De Seversky, *Air Power: Key to Survival* (New York, NY: Simon and Schuster, 1950), 193.
[51] Mitchell, *Winged Defense*, 436.
[52] J.C. Slessor, *Air Power and Armies* (1936; new imprint, Tuscaloosa, AL, Alabama University Press, 2009), 15.

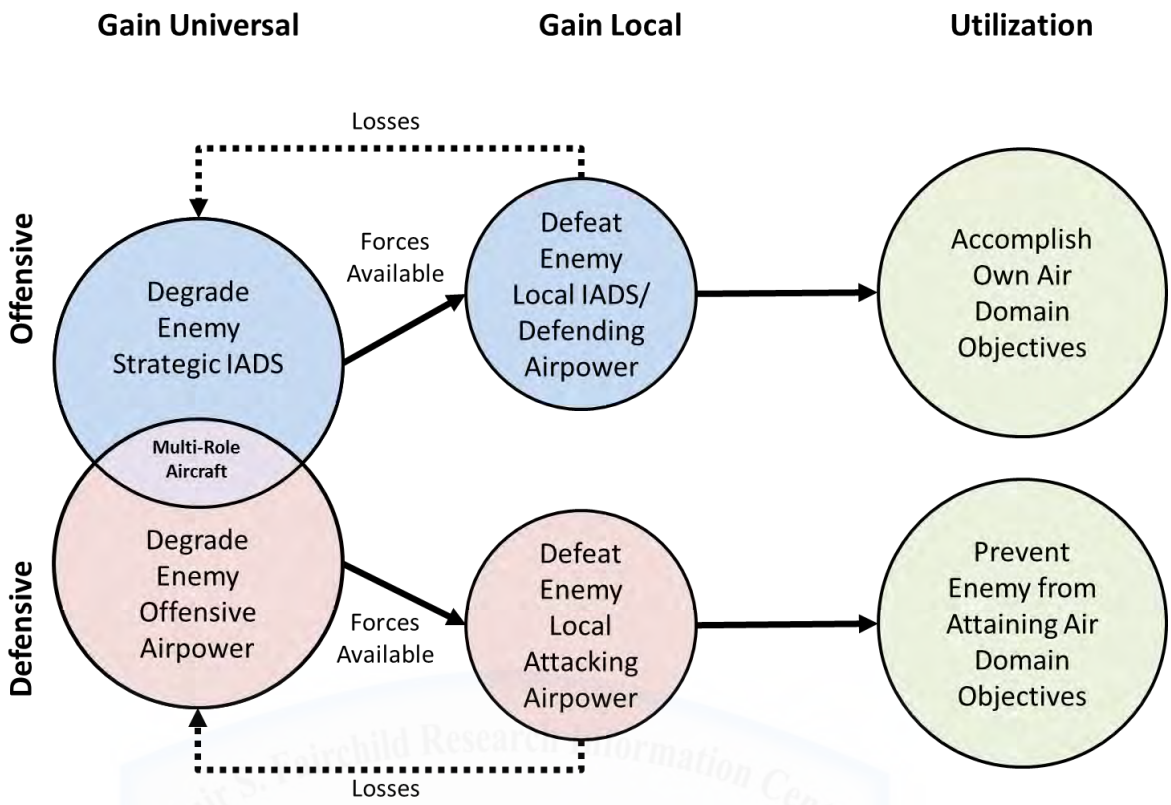

Figure 6 – Model of Gaining and Utilizing Air Superiority
Source: Author's Original Work

Note that there is some overlap between the offensive and defensive sides in the form of multi-role airpower. Multi-role aircraft can perform either defensive or offensive roles and so can swing between offensive missions and participating as part of the friendly IADS. The size of the overlap will vary depending on the forces available to a specific combatant. The next elements of the model relate local air superiority and universal air superiority.

The universal level of air superiority is more significant than the local level due to the excellent mobility of airpower, the concentrated capabilities of the airpower instrument and the vulnerability of universal airpower to attack. These factors are more important than the different offensive and defensive forces, which increase the

importance of the local level of air superiority. Airpower's long range and great speed greatly expands what constitutes a local area. Even short-range fighters can easily perform missions hundreds of miles from their airbases; with air refueling, they can go much further. At the logical extreme, if all aircraft could range the entire theater at great speed, there would be no local level as any air domain combatant could engage in any local combat.[53] The constraints of range and speed do not allow this collapse of the local level over large theaters, but the air domain comes much closer to this ideal than the land and maritime domains. The concentrated character of airpower also increases the significance of the universal level of air superiority.

The small numbers of air domain forces, combined with their vulnerability to attack further increases the importance of the universal over the local level of air superiority. Aircraft are generally much more expensive than tanks or artillery pieces so nations tend to have fewer of them. Aircraft are also fragile and easy to destroy, particularly if they are on the ground. Even the best shelters Saddam could buy provided minimal protection for the Iraqi Air Force during both Gulf Wars. The Israelis also demonstrated how the concentration and vulnerability of an air force could lead to universal air superiority when they destroyed the bulk of the Egyptian Air Force on the ground during the Six Day War. While the universal level is more important, the local level still matters in the air domain.

Local air superiority involves defeating only those enemy forces required to attain a specific objective in a local area whether that be offensive or defensive. The forces

[53] The projection that all aircraft would be able to range the entire theater is why Alexander de Seversky confidently predicted that local air superiority could not exist. Seversky was incorrect in this projection, and very few aircraft possess the range today that he predicted they would have by the 1950s and 1960s.

available to contest local superiority come from the universal level and losses taken in the fight for local superiority affect what forces are available for the next fight at the local level as was discussed earlier. On the local offensive side, a combatant has to defeat the enemy local IADS to be able to operate and accomplish objectives in the local area. Destruction of the entire IADS is not required; deception, disruption and denial are all options; an attacker can consider any of them as defeat of the IADS if the enemy IADS is unable to accomplish its mission of prohibitively interfering with the attacker. On the local defensive, the defensive side does not need to destroy the enemy's offensive airpower; it is sufficient for a defender to keep the enemy from attaining his offensive objectives. Of course, destruction is generally preferred, as those aircraft then cannot come back and attack again tomorrow. A combatant does not have to defeat enemy offensive airpower strictly with air domain forces, other domain forces can have key elements of that fight from ground or maritime based SAMs to cyberspace weapons implanted in enemy aircraft. Once air superiority is gained, the next question for a combatant is how best to utilize it.

Use of Air Superiority

There are three major ways that airpower analysts have suggested a combatant can use airpower to achieve his campaign objectives. The first is to attack some portion of the enemy population to get them to bring pressure on enemy decision makers to terminate the conflict on terms favorable to the attacker. The second is to attack infrastructure or industry to prevent the enemy from constructing weapons, and the third is to use airpower to support surface forces. There is often some blurring of the categories. For example, if the Allies knocked out a railway yard in Germany prior to the

Normandy invasion, it could conceivably have been putting pressure on the population, disrupting weapons production, and hitting troops headed to the front at the same time. Each of these mechanisms has a cyberspace equivalent and I will look at all three starting with direct attacks on the population.

The first proposed theory by which airpower could bring victory was direct attacks on the population, but this theory was largely discredited by the experiences of World War II. The earliest proponent of attacking enemy cities was Douhet, who considered attacking enemy vital centers the proper role of air domain forces.[54] Prior to World War II, many airpower advocates, including Douhet, thought that bombing would result in the collapse of enemy morale and end the conflict. Seversky disagreed on this point with Douhet even before World War II. During the war, and despite the utter devastation wrought by Allied bombers on many German cities, the Germans still did not surrender until their military had completely collapsed. In the Japanese case, even greater destruction did not bring surrender until after two nuclear weapons and the entry of the Soviet Union into the war. After World War II, Seversky stated that, "The morale of a nation determined to defend itself cannot easily be broken, especially in a national life or death struggle. Ideologically inspired people can withstand great amounts of punishment. It is never fear, horror, or misery which makes a people at war collapse but the actual elimination of the physical industrial means to make war."[55] This focus on industry leads to the next proposed mechanism for airpower of disrupting the industrial web of a nation.

---

[54] Douhet, *The Command of the Air*, 338.
[55] Seversky, *Air Power: Key to Survival*, 58.

A second theory for the proper use of airpower was that instead of destroying enemy cities and populations, bombers should destroy carefully selected "bottlenecks" in enemy industry, which would prevent the enemy from continuing to fight. A number of U.S. Army Air Corps officers on the faculty of the Air Corps Tactical School developed this theory during the interwar period.[56] The industrial web theory led to the U.S. Army Air Corps pursuing daylight precision bombing during World War II, but it was not as effective as its proponents had hoped due to a combination of the bombers being more vulnerable as well as less accurate, and the enemy more resilient than they expected. The shortcomings of daylight precision bombing led some analysts to conclude that the principal utility of air superiority was in support to surface forces.

A final concept for the proper use of air superiority was to utilize it to provide support to friendly surface forces. Some early airpower theorists such as Douhet and Seversky disagreed with this approach.[57] John Warden, a more modern airpower theorist, agreed with Douhet and Seversky and placed fielded military forces in the outside ring of his model.[58] On the other hand, among early airpower theorists, Mitchell recognized the importance of what happens on the ground and Slessor agreed that who won on the ground was determinative.[59] Robert Pape, a modern airpower theorist, postulated that the way for a combatant to coerce an enemy into submitting was by defeating their strategy,

---

[56] David MacIsaac, "Voices from the Central Blue: The Air Power Theorists," in *Makers of Modern Strategy: From Machiavelli to the Nuclear Age*, ed. Peter Paret (Princeton: Princeton University Press, 1986) 634.

[57] Douhet went so far as to state that, "For the rest, anyone who read Part I with attention must have understood perfectly that I considered auxiliary aviation *worthless, superfluous, harmful*." Douhet, *The Command of the Air*, 338. Seversky agreed with Douhet that action in support of the other services was a secondary function of airpower; the primary function was to strike directly at the enemy. Alexander P. De Seversky, *Victory Through Air Power* (New York, NY: Simon and Schuster, 1942), 264.

[58] John Warden, "The Enemy as a System," *Air and Space Power Journal* (1995), 46.

[59] Slessor, *Air Power and Armies*, 1.

but often the enemy strategy depended on the enemy's fielded military forces so attacking fielded forces could be the best way to defeat the enemy's strategy.[60] Airpower can have beneficial effects both by destroying targets deep behind enemy lines, as well as by attacking enemy forces directly on the front lines. Early airpower advocates were unnecessarily dismissive of attacks on fielded military forces because they were focused on "strategic" targets, but there are cases where the army is the most important "strategic" target since it is the force that the leaders rely on to keep themselves in power or accomplish their strategy. Each of these three approaches has some utility in cyberspace.

Cyberspace superiority aligns closely with air superiority in how combatants can use it; and cyberspace analysts should carefully consider the historical lessons from the air domain. Cyberspace strategists who propose approaches intended to pressure populations should seriously consider whether turning off power and water will put more pressure on a population than high explosive bombs and incendiaries did during World War II. It is possible that pressure strategies could work if the issue is of relatively low importance to the enemy, but the historical record of accomplishment from the air domain is not encouraging regarding such punishment strategies. Strategists should also be cautious when assuming they can successfully interfere with enemy industry and infrastructure based on airpower's experience with the industrial web theory. Cyberspace weapons may not be as effective as expected, and the enemy may be able to react in creative ways to mitigate the weapon's effects. Finally, the importance of using air

[60] Robert Pape, *Bombing to Win: Air Power and Coercion in War* (London: Cornell University Press, 1996), 17.

superiority to support the other domains also applies to cyberspace where, at the current time, cyberspace is likely to have the most impact. The utility to a combatant of achieving cyberspace or air superiority will also vary with how long he can expect to maintain that superiority.

Persistence of Air Domain Superiority

Because of the high mobility of air domain forces to move from one local area to another, a combatant will be able to achieve persistence of superiority in the air domain only if he is able to achieve universal versus local air superiority. The theorists who believed air superiority was persistent tended to also assume it was universal. Seversky was the most clear in his claim that there was no such thing as local air superiority when he said that, "Any attempt to conquer a small part of it—to protect a base underneath or for some other purpose—will rapidly resolve into a showdown battle for dominance in the air. Because of the enlarged ranges, mastery of the skies has come to mean *all* the skies."[61] Seversky reached this conclusion because he thought that all combat aircraft would be capable of ranging the entire theater of operations. If Seversky had been correct that all air superiority was going to be universal, his expectations about its long persistence would likely have also been correct. However, most aircraft did not achieve theater-wide range, which increased the importance of the local level of air superiority while decreasing persistence. In addition to the limited range of most aircraft, the creation of effective land based defenses also increases the relative importance of local superiority.

[61] Seversky, *Air Power: Key to Survival*, 58.

Modern IADS can break down a theater of operations into separate local areas in which different combatants have air superiority. If two nations went to war with non-cutting edge fighters and modern SAMs such as Patriots, SA-10s or SA-20s, it is reasonable to expect that both nations would be able to control the airspace above their own territory, while not being able successfully to penetrate that of the enemy without taking prohibitive losses. It is even conceivable that if the theater of operations were small, and both sides possessed effective long range SAMs such as the SA-12, neither side might be able to effectively utilize aircraft at all, even over their own territory. An even more common scenario is that a nation might have local air superiority in the areas where the most capable components of its IADS reach, but might not have air superiority in the areas outside their reach. Because aircraft can move so quickly from one zone into another, local superiority also tends to be transient.

Airpower theorists, who saw that air superiority could be local, also recognized that local superiority would tend to be transient. Soviet General P. P. Ionov believed that the air superiority that mattered would be both temporary and local. In addition, Ionov argued that he would be willing to trade universal air superiority for local superiority in a critical area.[62] Slessor, with a similar focus on land campaigns as Ionov, thought that air superiority was not a "condition to be achieved once for all."[63]

Seversky and Douhet, on the other hand, treated air superiority as persistent, once a combatant achieved it, the enemy would not have an opportunity to get it back because the victorious side would have destroyed the enemy's air force. Even Douhet had to

[62] Beatrice Heuser, *The Evolution of Strategy: Thinking War from Antiquity to the Present* (Cambridge: Cambridge University Press, 2010), 301.
[63] Slessor, *Air Power and Armies*, 10.

admit that localized air superiority was the best that either side achieved during World War I, although he attributed this shortcoming to the inefficiency of air-to-air combat as a method of gaining air superiority.[64] Douhet and Seversky were wrong because most combat aircraft did not have the range to affect the entire theater of operations, and air forces proved far more resilient and able to spring back from battlefield defeats. In World War II, the British and the Russians gained back air superiority despite tremendous early losses and air superiority was certainly not theater wide for any combatant until the final months of the war. The French Admiral Raoul Castex thought that the concept of permanent air superiority was absurd, as aircraft could only stay airborne for a short period.[65] Given the short endurance and high mobility of most current combat aircraft, the only way to generate persistent air superiority is at the universal level.

Air superiority will tend to be local and transient unless one side has such an overwhelming abundance of superiority that they can achieve it across the entire theater of operations as the Coalition did in the Gulf War. The primary reason for this situation is that a combatant can quickly move aircraft from one local area to another. Achieving dominance in a local area by destroying local air domain forces will only last until the enemy can move replacements into the threatened area and once again contest for superiority. An attacker could achieve slightly longer superiority persistence by attacking airfields or support equipment, but the enemy can also rebuild these in days or weeks through repair and reconstitution; or the enemy could still contest the local area using

[64] Douhet, *The Command of the Air*, 317.
[65] Heuser, *The Evolution of Strategy*, 302.

longer-range aircraft or air refueling. A more promising approach for a combatant is to utilize effective long range SAMs to establish local air superiority. However, if a combatant bases air superiority purely on these systems, the enemy will respond by focusing on them and air superiority will only last as long as those systems remain effective. As strategic theorist Edward Luttwak has observed, the more effective a system is, the shorter its utility tends to be as the enemy focuses on finding ways to defeat it.[66]

The tendency in the air domain for local superiority to be transitory has important implications for cyberspace superiority. Since universal superiority will be extremely difficult to achieve as will be discussed in chapter 3, the evidence from the air domain suggests that persistence of domain superiority will also be short in cyberspace. To understand how much air superiority a combatant has, I will next turn to how analysts have measured it over time.

Measurement Concepts of Air Superiority

If we accept Mitchell's definition of airpower or air superiority as, "the ability to do something in the air," then measuring it is a question of measuring how effectively an attacker or defender is accomplishing his or her objectives.[67] Common measurements include how often strike aircraft have to jettison their bombs before getting to their targets, how often targets are struck successfully, how many enemy sorties get into friendly territory and what was their effectiveness. A combatant can also utilize an

[66] Edward N. Luttwak, *Strategy: The Logic of War and Peace* (Cambridge, MA: Belknap Press, 2003), 28-29.
[67] Mitchell, *Winged Defense*, 425.

estimated balance of forces, but those measurements need careful scrutiny as nations produce airpower through a system, not from a single component. For example, a nation may have the best fighter aircraft on the planet, but if their pilots are substandard, they may not be very effective at projecting airpower. We can say the same thing about logistical systems, integration, munitions, etc. A combatant can utilize relative measurements; such as the fact that the enemy has lost 50% of his aircraft while you have only lost 10% of its own to determine which direction air superiority is going. Finally, actions by the enemy that demonstrate he has given up seriously contesting the air such as burying his planes in the sand, or flying them to a neutral country can be strong indicators that a significant level of air superiority or even supremacy has been achieved. Not all of these measurement concepts will transfer well to the cyberspace domain.

The core of assessing cyberspace supremacy will be measuring the accomplishment of a combatant's objectives similar to the air domain; however, measuring the balance of forces will be less useful. Estimating the balance of forces in the cyberspace domain is much more difficult than in the air domain. Air domain analysts can examine the number and types of aircraft available to each combatant, consider logistical and sortie generation capabilities, and examine infrastructure such as airfields relatively easily. In the cyberspace domain, a combatant cannot examine the enemy's weapons and infrastructure on satellite photos; they are much more difficult to find. In addition, matching the capabilities of an F-16 and a MiG-29 is relatively simple compared to determining the relative effectiveness of various cyberspace weapons. Cyberspace weapons are unique; how can an analyst compare a worm and an intrusion detection system? The focus on measuring objectives from the air domain I will carry

forward to construct a measurement concept in chapter 3 for cyberspace. Now we can summarize the findings from the land, sea, and air domains.

Conclusion

I can apply a number of different elements from the land, maritime, and air domains to the cyberspace domain. The geography and characteristics of each domain determine whether the offense or defense has primacy, how a combatant gains and uses superiority, the persistence of superiority, and appropriate measurement concepts for superiority. In each of these categories, there were major differences across the domains. While the land domain is the one least like cyberspace, there are still key elements I can bring forward into the cyberspace domain.

The principal elements of land superiority applicable to cyberspace include the interaction between universal and local superiority and how that interaction affects the persistence of superiority in the domain. In the land domain, a combatant can achieve universal superiority by defeating the enemy army, which can produce persistent superiority. If a combatant can only achieve local superiority, then persistence he can achieve tends to be much more fleeting. This point suggests that domain superiority in the cyberspace domain will be very short as it is very difficult to achieve anything other than local cyberspace superiority as will be discussed in chapter 3. A second critical element is that forces at the universal level of superiority control the forces available that a combatant can move into a local area to contest local superiority, and the losses at the local level feed back into what is available at the universal level. In all the other major

areas examined, land domain superiority manifests itself very differently than cyberspace superiority. The maritime domain has more areas of similarity to the cyberspace domain.

The maritime domain is similar to the cyberspace domain in that the primary purpose of the domain is to serve as a communication pathway. In the maritime domain, goods transit the sea lines of communications, in the cyberspace domain, information transits cyberspace. The maritime domain chokepoints such as straits and ports are analogous to cyberspace's chokepoints of undersea cables and server farms. Cyberspace will also likely be similar to the maritime domain in that the domain will normally be un-commanded as there will be so few domain forces to cover large areas in both domains. There is also potential utility in examining cyberspace conflict in terms of maritime commerce warfare. The maritime concepts of a fleet in being, fleet battles, and blockades do not have similar resonance in cyberspace. There is even more similarity between the cyberspace and air domains than the maritime domain.

The air domain is closer to the cyberspace domain than the maritime domain in its separation into mostly distinct offensive and defensive sides, its speed of action, reliance on technology, and the continuing debate on whether the most effective use of the domain is to target the enemy directly or support friendly action in other domains. The air domain differs from cyberspace in the cost of access and the importance of the universal level of superiority. Whereas the universal level is very significant in the air domain as combatants can easily attack universal air domain forces, in cyberspace it is much more difficult to attack enemy cyberspace forces. This circumstance results in far greater importance for the local level of domain superiority in cyberspace versus the air domain. In the air domain, a combatant can only achieve persistent domain superiority at

the universal level, which again implies that combatants will be unable to achieve persistence easily in cyberspace as it functions primarily at the local level. Finally, the measurement concepts from the air domain of focusing on the achievement of friendly objectives, while preventing the enemy from achieving his objectives will provide a starting point from which to develop a cyberspace measurement system. A summary of the findings for domain superiority across the land, maritime, and air domains are in table 1.

Table 1 – Summary of Domain Superiority for Land, Maritime, and Air Domains

Geography/ Characteristics	
Land	□ Physical terrain such as mountains, rivers, and swamps dictate lines of communication and which forces are most effective where □ Combat tends to be sequential with forces excluding each other from areas of their control while protecting their own lines of communication
Maritime	□ Maneuver space is bounded by land masses and ports which form chokepoints □ Sea lines of communication are the key element worth fighting over □ Accessed via expensive technology (ships) and expensive entry points (ports)
Air	□ Open and relatively unbounded without natural chokepoints □ No clear front line--involves civilians directly in combat operations □ Characterized by great speed of action □ Dependent upon technology for access □ Accessed via expensive technology (aircraft) and expensive entry points (airfields) □ Dominance in this domain is not sufficient for victory, however it enables the land and maritime domains
Offensive or Defensive Primacy	
Land	□ With modern weapons the defensive has primacy as the defender can stay under cover while the offender must unmask to advance
Maritime	□ There is no clear offensive or defensive primacy in the maritime domain o Normally both offensive and defensive forces can see

	each other at the same distance • Exceptions include submarine warfare which favors the offender and a fleet in a defended port which favors the defense
Air	• Older theorists favored offensive, but the advantage has shifted back and forth over time depending on technology
Method of Gaining Superiority	
Land	• Universal – Defeat enemy army to allow physical access to the terrain and then gain control and support of the population • Local – Defeat local regular or insurgent forces
Maritime	• Universal – Defeat enemy fleet or blockade them in port; weaker combatant can contest by keeping a "fleet in being" and executing small counter attacks • Local – Disrupt enemy shipping while protecting your own
Air	• Offensive universal – Degrade enemy strategic IADS • Defensive universal – Degrade enemy offensive airpower • Offensive local – Defeat enemy local IADS • Defensive Local – Defeat enemy local offensive airpower
Use of Superiority	
Land	• Often control of the land domain will terminate the conflict; if not, combatant can extract resources for continued combat in other areas and domains
Maritime	• Enable shipment of military and commercial goods • Project power into the land domain while preventing the enemy from doing the same
Air	• Offensive – Directly striking enemy centers of gravity to either affect enemy capabilities or change enemy decisions; Support other domain forces • Defensive – Prevent enemy from striking friendly centers of gravity
Persistence	
Land	• Land domain superiority tends to be persistent due to greater influence of the universal level of superiority as well as the sequential tendencies of land combat, the inertia of populations whose support changes slowly, and the current primacy of the defensive
Maritime	• Whether the maritime superiority gained is local or universal will greatly affect the persistence of maritime superiority ○ If a combatant can achieve universal maritime superiority through defeating the enemy fleet, then persistence can be high • If the enemy refuses to fight a major fleet action for universal control, then control will not only be localized, but also fleeting as the enemy can dash out of port to raid convoys and establish

	local control in an area, but then retreat back into port when threatened by the main adversary fleet
Air	Because of the high mobility of air domain forces to move from one local area to another, a combatant will be able to achieve persistence of superiority in the air domain only if he is able to achieve universal versus local air superiority
Measurement Concept	
Land	Whose soldiers are in possession of the terrain Metrics to determine the level of support of the population
Maritime	Universal – Remaining capability of enemy fleet Local – Metrics to measure friendly and enemy utilization of sea lines of communication; Ability to project power into other domains
Air	Ability to achieve objectives in the air Relative measurement and trends of resources

Cyberspace shares more characteristics with the maritime and air domains since both are domains accessed by technology. Accordingly, more of the characteristics of maritime and air superiority will be applicable to cyberspace. Examining the characteristics of the cyberspace domain in detail will be required to determine which characteristics cyberspace superiority and one of the other domains share. This analysis will then permit the addition of the cyberspace domain to table 1, which I will present at the end of the next chapter.

3 – CYBERSPACE DOMAIN CHARACTERISTICS & CYBERSPACE SUPERIORITY

In this chapter, I will examine the characteristics of cyberspace that are necessary to understand cyberspace superiority. Cyberspace is immensely complex and I will not attempt to explain all its aspects, but instead I will focus on those concepts necessary to understand how to gain cyberspace superiority and what a combatant can do with cyberspace superiority once gained. Chapter 2 laid out the characteristics of superiority in the land, maritime, and air domains, while this chapter will lay the foundation for an understanding of cyberspace superiority, enabling chapter 4 to build on that foundation to construct a system of measurement for cyberspace superiority. I will analyze cyberspace superiority by utilizing the same categories examined in chapter 2 for the land, maritime and air domains. I will examine the geography and characteristics of cyberspace, offensive or defensive primacy in cyberspace, methods of gaining cyberspace superiority, the use of cyberspace superiority, the persistence of cyberspace superiority, and measurement concepts of cyberspace superiority. A connecting strand throughout these categories will be the interaction between the universal and local levels of domain superiority.

In chapter 2, I showed that we could analyze domain superiority at both the universal and local levels; while there is a universal level of superiority in cyberspace, the local level will be dominant. This dominance is due to a number of factors I will explore in this chapter including the uniqueness of offensive and defensive cyberspace forces, the difficulty of attacking cyberspace forces at the universal level, and the dispersed

character of cyberspace forces. To build this argument, I will first examine a few of the characteristics of cyberspace as a domain.

Geography and Characteristics of Cyberspace

Cyberspace is composed of information and connections in a virtual space, but it is grounded in the physical world. According to cyberspace analyst Paul Rosenzweig, "we should never forget that though the cyber domain is an artificial one created by man, it exists only in the context of the fundamental natural domain of the world."[1] Events in the physical world affect cyberspace. If the heart of cyberspace is the connections between computing devices, then anything that affects those devices or their connections affects cyberspace. A failed air conditioning unit at a server farm, a backhoe cutting a fiber cable, or an anchor dragging across an undersea cable can have a tremendous impact on cyberspace. These links and connections to the physical world can provide attackers seeking cyberspace superiority important levers to utilize. Before delving into methods of gaining cyberspace superiority, it is helpful to consider a model of cyberspace that illuminates why cyberspace superiority operates the way it does.

Model of Cyberspace

There are numerous models of cyberspace, and many of the models share common characteristics. The earliest layered model that analysts have applied to cyberspace is the well-known Open Systems Interconnection (OSI) seven-layer model of a communication system. The OSI model starts with the physical then moves through data link, network, transport, session, presentation, and application layers. I find it less

[1] Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World* (Santa Barbara, CA: Praeger, 2013), Kindle Location 488, chap. 2.

useful in analyzing cyberspace superiority than other models as it focuses only on the communication system and does not adequately separate the information from the information carrying system. How one models information, versus the system on which it travels, is a critical concept in cyberspace superiority.

The U.S. Army Training and Doctrine Command (TRADOC) proposes that analysts can best understand cyberspace in three layers with five components. The layers are the physical, logical, and social. The physical layer includes both the geographic and physical network components, while the logical layer includes only the logical network component. The social layer has two components, the persona and cyber persona components.[2] The persona component is composed of actual people, while the cyber persona is composed of cyberspace identities. Thus, a single person can have multiple cyber personas (such as multiple e-mail accounts) and a single cyber persona can be made up of multiple people (such as an organizational e-mail account.)

I find that the social layer of the TRADOC model is problematic from a cyberspace superiority perspective. The social layer consists of real people in the form of persona components, and virtual people in the form of cyber persona components. Cyberspace superiority is about achieving objectives through the domain of cyberspace. If people are included in the model, then the distinctiveness of the domain starts to break down. Influencing people through cyberspace is something you do with cyberspace superiority; it is not cyberspace superiority itself. Like the OSI model, I find this model lacking in not separating information from the information system. Another issue with

[2] TRADOC Pamphlet 535-7-8, *The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028*, 22 February 2010, 8.

the model is that TRADOC defines the logical layer to consist of network devices such as routers and so this layer conflates with the physical layer, which I do not find helpful

David Clark from MIT has offered a model with four layers. The bottom layer is the physical foundations, next is logical building blocks, then information, and finally people.[3] Clark views cyberspace as hierarchical with people at the top connecting through information to logic to the physical foundations of cyberspace. Clark also states that cyberspace can be thought of as a "think veneer" drawn over the real world, rather than a separate world or space.[4]

I find Clark's model to have several helpful elements, especially in the distinction made between logical building blocks and information as separate layers. However, the people layer brings confusion into what is part of the cyberspace domain and what is not, which is not helpful as discussed earlier. All of these models include a physical and some sort of network or logical layer, but they differ in the higher layers. However, there is a model more applicable to understanding cyberspace superiority.

Libicki's description of cyberspace is the most helpful, especially in the context of cyberspace superiority. Libicki builds his model using an analogy from linguistics and breaking cyberspace into the physical, the syntactic, and the semantic.[5] The physical layer consists of the wires, routers, and computers that create cyberspace and is the foundation of the model. The syntactic layer consists of the rules by which cyberspace actors move and process information in cyberspace. The software of cyberspace, both

[3] David Clark, "Characterizing cyberspace: past, present and future" MIT CSAIL, Version 1.2. 12 March 2010, 1.
[4] Clark, "Characterizing cyberspace: past, present and future," 5.
[5] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007), 5.

operating systems and applications, normally represents this layer. The final layer is the semantic layer. The semantic layer is the information itself. All three layers must work together for cyberspace to function.

As a simple example of how the three layers interact, consider a user opening a web browser to view "cnn.com." The initial input will come into the system at the physical level through a mouse and keyboard. At the syntactic level, the computer will interpret the input by utilizing the rules in the operating system. The operating system then uses the physical level to send the request through the network card to a router whose syntactic rules seek out the information and return it to the computer. The computer then displays the semantic information via a syntactic web browser on a physical monitor. The three-layer model can be viewed as a pyramid as in figure 7.

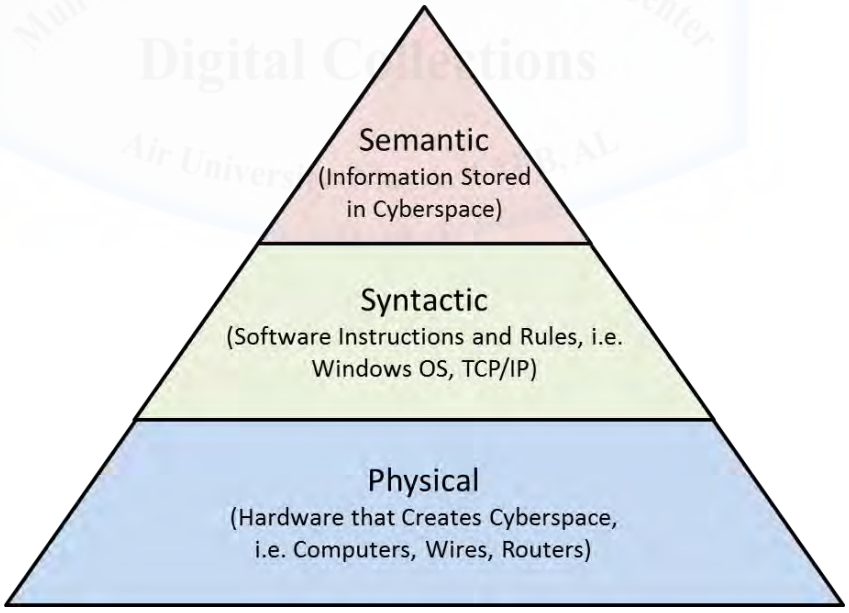

Figure 7 – Libicki's Model of Cyberspace
Source: Adapted from Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007), 5.

Each higher layer of the model is dependent on the lower layers; if the lower layers fail, the higher layers also fail. The syntactic layer is dependent on the physical layer and the semantic layer depends on the syntactic. Elimination of the physical layer would cause the syntactic and semantic layers to dissolve, but the converse is not true. If a completely effective semantic attack deleted all the information in a database, it would not affect the syntactic and physical layers. If a backup of the information exists, which is increasingly common due to reduced storage costs, then one could rapidly reconstruct the semantic layer using the still intact syntactic and physical layers. The same is true of the syntactic layer. If a syntactic attack completely erases the operating system, but leaves the physical hardware untouched, it is much easier to reconstitute than if an attacker destroyed the hardware itself. While the layers interact, their different characters require different approaches for combatants seeking cyberspace superiority.

Each of the three layers is part of the struggle for cyberspace superiority; however, as identified by Libicki, combatants attack and defend them in very different ways.[6] If a combatant can cut communication links, or destroy cyberspace components in the physical realm, that does not imply any ability to manipulate the operating system, or the information stored on the system. Likewise, a combatant who can manipulate the data flowing into, or stored in, a system has not automatically gained the ability to change the rules by which data is stored and managed. A combatant must attack or defend cyberspace in ways that are unique at each level with the physical layer being the most obvious one.

[6] Libicki, *Conquest in Cyberspace*, 9.

Within the physical layer, an attacker can attack the hardware of cyberspace such as cable repeaters, fiber optic cables, or even the human component by attacking cyberspace operations personnel. Physical attacks can come through any of the physical domains or the cyberspace domain itself. As engineers demonstrated in the Aurora test, a cyberspace attack can physically destroy a generator.[7] There are also ways that a cyberspace attacker can target computing devices on the physical level. One technique is to rewrite the cooling protocols to generate a physical failure of the processor. The defender will respond to these types of attacks utilizing whatever domain forces are available and appropriate. Physical security of installations, air defenses, and isolating systems via an "air gap" provide some of the common defense on this level.[8] Moving from the physical to the syntactic level is where an attacker enters the realm of software versus the physical hardware.

Software and operating systems reside at the syntactic level and offenders normally attack them through errors in the code that allow an attacker to trick a computer system into executing a set of instructions sent by the attacker. The syntactic level is what most people think of when discussing cyberspace attack. This layer is the home of protocols such as TCP/IP, operating systems, and applications. Attacks on this level include software Trojans, utilizing software flaws, and denial of service attacks.[9] Defenses include firewalls, intrusion detection systems, and patching vulnerabilities. It is

[7] Paulo Shakarian, Jana Shakarian and Andrew Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach* (Amsterdam: Syngress, 2013), Kindle Location 6561, chap. 12.
[8] Air gaps are networks that designers have not physically connected to the Internet or other networks as there is a "gap of air" between them. This is a common and generally effective way of protecting important systems, but it does have some limitations and weaknesses, as I will discuss later. A more detailed description of air gaps and other defenses is in appendix C.
[9] For a description of these types of attacks and others, see appendix C.

important to note that this level deals with the rules and processes by which computing devices handle the information, not the information itself. This distinction is critical to understanding cyberspace attacks and defense. Libicki draws a clear line, "between *attacks on information* and *attacks on information systems.*"[10] He also notes that,

> …those who would attack the mind of the enemy by attacking information systems may succeed in making much of what the enemy knows inaccessible, but not necessarily by changing the content of the information itself. It is akin to claiming that one has successfully messed with someone's mind by giving him or her a headache.[11]

If an attacker is trying to change the information itself, he or she has moved onto the semantic level.

The semantic level is where the actual information lies and combatants attack on this level by manipulating, destroying, or even adding information. The semantic level is where most information operations take place.[12] An attacker can destroy or manipulate information at rest by attacking information storage; he can also attack information in motion by disrupting communication systems.[13] Examples abound of ways to implement this type of attack at the semantic level.

---

[10] Libicki, *Conquest in Cyberspace*, 23.
[11] Libicki, *Conquest in Cyberspace*, 24.
[12] According to Joint Pub 1-02 information operations is, "The integrated deployment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own." Department of Defense, *Joint Publication 1-02*, 15 December 2012, 140. Operations in the cyberspace domain will often contribute to information operations, but operations that have physical effects such as taking down a power grid will not. Some information operations will not be in the cyberspace domain such as dropping pamphlets from aircraft. There is overlap between information operations and cyberspace operations, but there are exclusive areas as well.
[13] Libicki has identified that there are many other ways to attack information as well. An attacker can attack the credibility of enemy information by injecting false information that will call into question the veracity of the rest of the information the enemy has. More subtly, given the difficulties most organizations and decision-makers have in successfully filtering information, an attacker could inject large quantities of factually correct, but low-grade information into the enemy system to bury important information under an avalanche of trivia. An attacker who cannot directly manipulate the information possessed by an adversary

There are many ways for a combatant to attack information and several avenues of defense at the semantic level. Examples include altering intelligence to mislead, corrupting logistical databases, changing manufacturing processes to induce flaws in equipment, etc. The possibilities are endless and limited only by the imagination of the attacker. Defenders have several avenues of defense to these attacks; they can boost the signal-to noise ratio, strengthen the signal through redundancy, or weaken the noise through filtering.[14] Examples of these defenses include keeping backups of databases and comparing them, utilizing multiple sources of intelligence with crosschecking, as well as data checking and verification processes. The key to a successful attack at the semantic level is that, "it relies more on the victim's predisposition to believe something then on the technical power to simulate that something convincingly."[15] One of the more famous examples of deception is the successful Allied campaign of World War II to convince Hitler that the European landings would be at Calais, not Normandy. The plan succeeded because the Allies were providing false evidence to reinforce what Hitler was inclined to believe already. This sort of information warfare is extremely difficult and requires an understanding of enemy leaders and their decision-making processes that will

---

may be able to raise the level of noise in the system and thus still degrade enemy decision-making. Libicki, *Conquest in Cyberspace*, 124.

[14] Libicki, *Conquest in Cyberspace*, 55.

[15] Libicki, *Conquest in Cyberspace*, 55.

normally be hard to acquire, although the equipment used to execute the attacks may be very inexpensive.

Cost of Entry into Cyberspace

An entry-level capability for a nation-state in cyberspace can be very economical; however, significant capability is still expensive. Combatants access the physical domains of maritime, air, and space by technology and do so as well in cyberspace. However, while the cost of ports, ships, airfields, aircraft, and spacecraft are very high, all a combatant needs to connect to cyberspace is an inexpensive computing device that he has connected to an Internet Service Provider (ISP). The entry costs into cyberspace are so low that collectives of civilians, such as Anonymous or even individuals, can become significant actors.[16] Libicki notes that while armored warfare normally is beyond the reach of private individuals and rogue tank units are easy to spot, the tools of cyberspace warfare are available to anyone and easily hidden.[17] When acting on their own, non-state actors are more of an irritant than a significant threat to nation-states; however, they can be more threatening when used as part of a broader nation-state cyberspace conflict.

Several nations have utilized so-called "patriotic hackers" as proxy forces, which made them important in interstate conflict. As I will discuss in the case studies, there is good evidence that Russia used "patriotic hackers" in support of state objectives in the conflicts in Georgia and Estonia. Chinese "patriotic hackers" have also been very active and while the evidence of links to the government is not as clear as in the Russian case; it

[16] Anonymous is a well-known international "hacktivist" group associated with numerous cyber attacks.
[17] Libicki, *Conquest in Cyberspace*, 257.

is reasonable to assume that there is some level of connection between the government and the hackers. China has exceptionally robust control of cyberspace inside China, and they have, at a minimum, chosen not to interfere with groups who were executing attacks aligned with Chinese objectives. While these groups represent a low cost entry into cyberspace conflict for a nation-state, their capabilities are limited. To develop and field cyberspace capabilities that could challenge a technically advanced nation-state for cyberspace superiority is very expensive.

While cost of entry is low, significant capability in cyberspace is not cheap and requires substantial expenditure of resources. Despite the romantic Hollywood appeal of a brilliant hacker in a basement taking on and beating the CIA or NSA, it is not likely to happen. An analysis of Stuxnet, for example, has shown that it would have taken approximately ten man-years to write and develop.[18] A single individual or even a small team did not write Stuxnet. Actually, the ten man-year estimate is low because it does not include the immense amount of detailed intelligence work that must have occurred prior to writing Stuxnet, or the extensive testing alleged to have occurred at various sites.[19] A cheap laptop and an Internet café will get you into cyberspace, but a substantial offensive or defensive capability is still something that is principally only accessible to nation-states due to the resources required. The expensive resources for success in cyberspace warfare require the abilities of many skilled people.

[18] Sean Sullivan, "Stuxnet Redux: Questions and Answers," *F-Secure*, 23 November 2010. http://www.f-secure.com/weblog/archives/00002066.html.
[19] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Broadway Books, 2013), 192.

It seems counter intuitive for a domain that derives its very existence from technology, but well trained and capable people are more important in the battle for cyberspace superiority than equipment. A cheap laptop, sold for less than $500, almost as a commodity, has more computing power than the "supercomputers" that used to fill entire rooms and cost millions of dollars only a few decades ago. In certain areas, such as cryptography, technology and computing power can be significant, but in many areas of cyberspace superiority technology is not the most important component. What brings success is people, and not just any people. According to Libicki, "Success at hacking requires daring, initiative, and the rapid identification and seizure of fleeting opportunities."[20] These cyberspace warriors are operating in a domain with a networked structure, which has implications for cyberspace superiority.

Additional Cyberspace Characteristics Relevant to Cyberspace Superiority

The network structure of cyberspace gives it a high level of built-in resiliency to attacks that focus on interfering with communication between nodes. When a computer sends information from point to point in cyberspace, the sending computer splits it into small pieces called packets that the computer sends separately for the receiving computer to reassemble into the complete message. These packets flow along the quickest logical, not physical, pathway between the two computers. An e-mail sent to your next-door neighbor, may flow geographically a very long way before ending up in his inbox, especially if he uses a different Internet Service Provider (ISP). The routers that manage Internet traffic exchange information about how quickly they are transmitting traffic

[20] Libicki, *Conquest in Cyberspace*, 257.

based on data load and environment. The routers then use that information to determine the fastest pathway for a packet of data, which can send a packet from Los Angeles to Denver through Miami. If an attacker were to interrupt a pathway from point to point, it is likely that no one would even notice, as packets would simply flow around the disabled communications node. If packets are lost when an attacker takes down a node, the receiving computer will automatically request the missing packets from the sending computer, which will flow via different channels and the complete message will still get through. This network character of cyberspace gives it substantial built-in resilience, which makes it much harder for attackers to interrupt or modify information in transit. Although cyberspace is a network, it is not evenly distributed and there are places where multiple communication pathways converge.

There are chokepoints in cyberspace that we can consider as roughly analogous to mountain ranges or other features in the land domain. Rattray likens cyberspace nodes such as undersea fiber optic cables or communications satellites to mountain passes in the land domain or straits in the maritime domain.[21] If an attacker disrupted these chokepoints, it could have a major impact on cyberspace superiority. As a result, these chokepoints may become the focus of battles for cyberspace superiority. If a combatant can control them, he or she is well on their way to gaining cyberspace superiority. An example of a constructed chokepoint is China's "great firewall." China has deliberately set up their Internet infrastructure so that there are only three major entry points.[22] An analogy from the land domain might be a nation surrounded by an impassible mountain

[21] Rattray, "An Environmental Approach to Understanding Cyberpower," 268.
[22] Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly*, Spring 2011, 42.

range that has only three passes connecting it to the outside world. It is much easier for the Chinese to control traffic through the three cyberspace "mountain passes" than it would be if there were hundreds or thousands of connections to other countries. China has created these limited entryways in an attempt to control communication in China, but there is also a down side as there are only three major connections into or out of China that an adversary needs to attack to cut China off from the rest of cyberspace. These chokepoints are not as static as mountain passes; combatants build them, and can change them far more quickly than in the other domains.

There are two facets to cyberspace's changing geography over time. First, combatants can connect, disconnect, or change the linkages between the components that create cyberspace. Every computer, router, or device attached, or removed, from cyberspace changes the cyberspace domain as a whole. We can think of an individual computer coming online as another grain of sand on the beach, one more or less grain of sand is not going to make much of a difference in the overall environment. However, much more significant changes are also possible. Rattray states that while mountains and oceans cannot be moved by combatants, in cyberspace a combatant can move or even turn off the equivalent geographic features quickly.[23] Someone does not even have to throw the switch deliberately; communications officers often joke that the most effective cyberspace weapon is a backhoe in the hands of someone who does not know where the utility company buried the cables. As an example, in 2008, a ship anchoring in the wrong spot severed 75% of the communications between Europe and the Middle East, and that

[23] Rattray, "An Environmental Approach to Understanding Cyberpower," 256.

incident was not nearly as significant as the 2006 earthquake that damaged seven undersea cables near Taiwan.[24] The chokepoints discussed previously represent nodes where physical disruption can produces major degradation and represent particularly vulnerable targets for combatants to attack and defend.

The second facet of cyberspace's changing geography is that designers rapidly continue to make the individual hardware more capable. Not only is cyberspace expanding as engineers connect more components, each new upgraded component can process faster, handle more connections, and store more data than the older ones. Computing power has risen at an exponential rate while storage costs have plummeted even faster.[25] Computers can process, move, and store amounts of data that were nearly inconceivable a few years ago. This fact has significant implication in the fight for cyberspace superiority as it makes it much more realistic to have multiple redundant computer systems that a defender can substitute for systems an attacker has disabled. Hardware redundancy has become far less cost prohibitive than in the past. As hardware becomes more capable and cyberspace expands, no nation will have superiority over the majority of cyberspace, the universal level of cyberspace.

Because of the small number of cyberspace forces in relation to the vast amount of cyberspace, normally no nation state will have superiority in a given area of cyberspace. Most of cyberspace is open and not directly controlled or regulated by any nation state. There are also no border guards and customs posts as cyberspace

---

[24] Elham Nakhlawi, Mustafa Al Arab, Caroline Faraj, Tess Eastment, Aneesh Raman and Brad Lendon. "Third undersea Internet cable cut in Mideast." *Cable News Network,* 1 February 2008. http://www.cnn.com/2008/WORLD/meast/02/01/internet.outage/.
[25] Rosenzweig, *Cyber Warfare*, Kindle Location 2248, chap 12.

communications cross borders. Lonsdale believes that because of its open nature with few forces similar to the maritime domain, Corbett's concept of no-one having superiority in the majority of cases will also apply to cyberspace.[26] This concept also implies that cyberspace superiority will generally trend towards neutral in the absence of significant effort by one side or the other, which will also limit the amount of superiority that a combatant can gain and how long a combatant can hold it.

Like the maritime, air, and space domains, analysts increasingly see cyberspace as a global common. According to NATO, "The Global Commons comprise four domains: maritime, air, space and cyber."[27] McCarthy concurs that "almost all modern scholarly analysis" includes the cyberspace domain as a global common and further illustrates the key element of a global common as, "that these areas are unowned and that no one nation is capable of exercising sovereignty over them in a manner that denies global access to the domain."[28] Despite the attempts to define cyberspace as a global common, it is not a settled question.

The argument that cyberspace is a global common seems to run counter to the fact that someone owns every piece of equipment that creates cyberspace, and every component physically exists in some country under a set of local laws. The argument in favor of cyberspace as a global common is that the cyberspace that emanates from these devices is not "owned." It is not my intention to settle this debate, but the growing concept of cyberspace as a global common can restrain what attackers choose to do in cyberspace.

---

[26] Lonsdale, *The Nature of War in the Information Age*, 185.
[27] Barrett, et al., "Assured Access to the Global Commons," 5.
[28] McCarthy, "Traveling Domain Theory," 61.

Combatants may restrain themselves in cyberspace to avoid crossing perceived global norms of cyberspace as a global common. For example, a cyberspace defender may want to disable computers that are attacking his systems. However, the attacker does not likely own those computers, but unaware, neutral third parties own them. If the defender disables them, is that akin to a naval combatant sinking neutral shipping on the high seas? Attackers may choose not to take actions that will move international public opinion against them. Another factor that cyberspace operators must consider is the inability of cyberspace weapons flexibly to engage enemy cyberspace forces.

Offensive cyberspace weapons have no ability to detect enemy offensive cyberspace weapons and so they cannot destroy them in opportune "meeting engagements."[29] If cyberspace weapons happen to cross paths in cyberspace, each will go right past one another with each heading on to its destination.[30] Cyberspace weapons do not have any ability to adapt to changing circumstances; they are more like an artillery shell fired by a cannon than a manned aircraft or ship that can choose to engage any enemy they find. This characteristic of cyberspace weapons makes the idea of offensive counter cyberspace from cyberspace unlikely to be useful.[31] Attacking an enemy's offensive cyberspace capability from one of the other domains is much more promising if you can cause physical destruction. A Joint Direct Attack Munition (JDAM) dropped on

[29] In a meeting engagement, both forces are moving forward and engage each other as soon as one side detects the other. These engagements are common in the land, maritime, and air domains. An example would be two opposing fighter aircraft that detect one another and engage despite the fact that they are both on bombing missions.
[30] Butler, "Refocusing Cyber Warfare Thought," 51.
[31] Offensive counter cyberspace is a USAF doctrinal concept where cyberspace forces go out, find, and destroy opposing cyberspace forces. It is drawn directly from offensive counter air, which makes much more sense in the air domain. An attack on an enemy airfield is an example of offensive counter air; it is difficult to find realistic equivalent missions in cyberspace that only involve cyberspace forces.

the building housing the enemy's cyberspace warfare center is an example of one possibility. This inability of cyberspace weapons to target each other as they cross in cyberspace is one of several reasons why the offense currently has the advantage in cyberspace.

Offensive or Defensive Primacy in the Cyberspace Domain

In the land domain, attackers are normally out in the open and susceptible to attack; however, in the cyberspace domain it is the defenders who are visible and open to attack. This situation is the fundamental reason why the offensive has the advantage in the cyberspace domain. However, as I will discuss later in the persistence section, this predominance tends to be short lived and only lasts until the defender feels the effects of the weapon and detects the offender. The differences between offensive and defensive tools in cyberspace also heavily influence cyberspace superiority.

Attackers and defenders in cyberspace rely on fundamentally different weapons and tools for offense and defense, similar to the air domain. In modern air combat there is a difference between offensive air power and ground-based defenses. A modern Integrated Air Defense System (IADS) utilizes ground based Surface to Air Missiles (SAMs) and Anti-Aircraft Artillery (AAA), surveillance assets integrated with Command and Control (C2), and airborne fighters. With the exception of multi-role fighters, these ground-based defenses cannot perform offensive missions into enemy territory; they can only target incoming aircraft. There is a similar difference between the defense and offense in cyberspace where offensive and defensive systems are not similar or interchangeable.

In the cyberspace domain, offensive and defensive weapons are not interchangeable, unlike the weapons of the maritime and land domains. At sea, a surface combatant such as a destroyer can perform either offensive or defensive missions. Even though there are specialized platforms such as submarines and anti-submarine aircraft, they normally can perform offensive or defensive missions. This flexibility of forces also exists in the land domain as tanks and infantrymen are just as important in the offensive and defensive roles. In the cyberspace domain, on the other hand, a firewall and a worm are fundamentally different and while both are important, are no more interchangeable than a Patriot and a B-52. Another way that cyberspace weapons are different from weapons in the maritime and land domains is that designers intend many of them to attack the target from the inside.

Cyberspace weapons can be thought of in two broad categories, those that attack from outside enemy systems, and those that attack from inside. Outside attacks focus on disrupting an enemy system's communication or access. The most common form of these attacks today are Distributed Denial of Service (DDoS) attacks where an attacker gains control of numerous neutral systems and then utilizes them to flood an enemy system with requests that prevent the enemy system from operating effectively. Other types of cyberspace based external attacks are attacks on supporting infrastructure for the targeted system such as attacking power or cooling. These attacks might be internal to the power control system, but they are external to the actual target. For example, consider a cyberspace attack that causes the cooling system for a server farm to heat up the server room to the point that the servers fail. It was an internal attack to the cooling system, but an external attack to the server farm. Less sophisticated and capable

attackers generally utilize DDoS attacks; an attacker can achieve greater effectiveness by getting inside enemy systems.

Offensive cyberspace weapons striking the inside of an enemy system attack in a two-stage process, first they gain access, and then they execute the mission. There are several ways that an aggressor can achieve access into an enemy system. The most common is through deception, where an attacker tricks a user into providing access. The normal method of accomplishing this is through an e-mail with an innocent looking attachment or link that opens the door for the attacker to get into and establish control of a system. Other potential avenues of access for an aggressor include software flaws, supply chain attacks, or software Trojans.[32] This first stage of the strike will look the same whether the attacker intends to take down a national power grid, or quietly look for intelligence. Thus it is hard for defenders to know what type of attack they are under until the, "cyber payload 'explodes' and the effects are felt."[33] In both stages of an internal attack, an offensive weapon tries to hide from the defender.

Most cyberspace weapons rely on deception to get in, and stealth to persist and accomplish their missions. Deception involves pretending to be something you are not; stealth involves attempting to keep defenders from seeing you at all. Cyberspace wolves may wear sheep's clothing to get into a system; but once there, they attempt to disappear completely. It is normally easy for a cyberspace weapon to hide within the millions of lines of code resident in a typical computer. Until a weapon does something that draws attention to itself, system administrators rarely find it. Attackers can design their

[32] For full descriptions of these types of attacks, see appendix C.
[33] Rosenzweig, *Cyber Warfare*, Kindle Location 511, chap. 2.

weapons carefully to remain hidden. Stuxnet is a famous example of a weapon that went out of its way to hide its presence by making the failures of the Iranian centrifuges look like mechanical and design failures instead of the result of a cyberspace attack.[34] This reliance of cyberspace weapons on hiding has several consequences.

Because most offensive cyberspace weapons rely on stealth and deception, defenders will generally be unable to see them coming, which gives an advantage to the offense. Unlike an infantry assault across an open field or an airborne strike package identified by radar, the first indication for a defender that an attack is underway may be the cyberspace weapon "going off." To remain hidden, attackers can utilize vulnerabilities that are unknown for new attacks. Analysts refer to cyberspace attacks that utilize unknown exploitable flaws as "zero day" attacks, because the timer on the vulnerability starts at zero when the defender discovers the attack and then increments up as software engineers scramble to develop a patch. Defenders who are unaware of the specific vulnerability will be unable to patch their system to eliminate the vulnerability. That is why zero day exploits are so important and guarded so carefully when discovered. Hackers often consider them the "crown jewels" and they can get prices of $50,000 to $500,000 on the black market for an exploitable Window's vulnerability.[35] Cyberspace defenders are unable to see attacks coming before they arrive; and they are often unable to determine where an attack came from after the defender discovers it.

The difficulty of attribution in cyberspace makes it challenging for defenders to understand where an attack is coming from and makes defensive responses more

[34] Barrett, et al., "Assured Access to the Global Commons," 41.
[35] Sullivan, "Stuxnet Redux: Questions and Answers."

difficult. At the current time, it is fairly simple for actors in cyberspace to remain anonymous with widely available tools. The designers of the Internet built it to be open and they emphasized communication over security and attribution. As a result, while covert operations are difficult and rare in the physical world, they are the norm in cyberspace.[36] Fortunately for defenders, difficult does not equate to impossible and defenders have some ability eventually to attribute attacks.

The anonymity of cyberspace is not absolute, even if the attackers are well resourced and competent. In the "Gh0stnet" attacks, an investigative team was able eventually to determine that the attack on the Dali Lama's network originated in China, but it took a year of effort.[37] In the battle for cyberspace superiority, knowing who did it a year after an attack may not be very useful, however sometimes attribution is apparent from the context of the attack. For example, in 2007 the Syrian air defense network went down due to a cyberspace attack. The fact that the cyberspace attack happened at the exact same time that Israeli fighter aircraft crossed the border to strike a suspected nuclear facility produces a reasonable level of confidence that the Israelis were behind the attack.[38] Sometimes attribution may be good enough for a nation to choose to respond even if the evidence is not strong enough to convince the international community. Of course, a nation has to be careful that they do not get into a fight because someone made it look like a regular or suspected enemy attacked. The difficulties with attribution suggest that combatants need to be cautious in assuming from where an attack

[36] Robert Belk and Matthew Noyes, "On the Use of Offensive Cyber Capabilities" (Master's Thesis, Harvard Kennedy School, 2012), 16.
[37] Rosenzweig, *Cyber Warfare*, Kindle Location 4630, chap. 21.
[38] Aki J. Peritz, and Michael Sechrist, "Protecting Cyberspace and the US National Interest" (Harvard Kennedy School Belfer Center for Science and International Affairs, 2010), 5.

is coming. This hesitancy to act can provide further advantage to the attacker in cyberspace.

The advantage in the cyberspace domain goes to the attacker who can be proactive, as he can remain hidden and anonymous, while the defender is out in the open and reactive. The ability of attackers to hide their origin increases this advantage, but does not make it absolute. Both the offense and defense will have a role to play in gaining cyberspace superiority.

Method of Gaining Cyberspace Superiority

In this section, I will analyze various concepts on how to gain cyberspace superiority from different authors and then build a model using elements of several authors as well as the insights gained from the other domains in chapter 2. Before moving to theories of gaining cyberspace superiority, I will first analyze some of the arguments analysts have made that cyberspace superiority does not exist or is not useful. I will start with those authors that are most critical of the usefulness of cyberspace superiority before moving on to those who see greater utility in the concept.

Libicki is a well-known cyberspace author who does not see much utility to cyberspace superiority and writes that the entire question of cyberspace superiority is meaningless and not a proper goal for cyberspace operators.[39] He believes that cyberspace superiority is impossible because combatants can simultaneously keep each

[39] Libicki, *Cyberdeterrence and Cyberwar*, 141.

other off their networks and believes that it is not useful to state that a hacker "controls" a system when the defender still has physical control.[40]

There are two reasons why I think Libicki is mistaken and there is utility to cyberspace superiority. First, the fact that combatants can simultaneously keep each other off their networks is a reflection of the different weapons and tools utilized by the defense and offense in cyberspace. This observation does not invalidate the concept of cyberspace superiority; it merely means that an analyst needs to examine two dyads instead of just one. An analyst needs to consider Nation A attacking nation B alongside nation B's attacks on nation A. This examination becomes most important when developing a measurement construct.

Second, I do not find Libicki's argument about physical control to be compelling. If a combatant "owns" his cell phone by right of physical possession, then does he still "own" it if it is working for the enemy? That cell phone could be reporting every private conversation, every e-mail or text, and providing the coordinates for the guided bomb about to land on the cell phone's owner. The physical owner may "own" the cell phone but if someone else controls and exploits it, the attacker would have meaningful cyberspace superiority according to the definition. A second author who is skeptical of cyberspace superiority is Sean Butler.

Butler has written that cyberspace superiority is not a useful doctrinal term as planners do not design campaigns to achieve it, and cyberspace superiority then ends up

[40] Libicki, *Cyberdeterrence and Cyberwar*, 141.

as merely a "shallow descriptor" of the quality of the engaged forces.[41] Butler thinks that a measurement of cyberspace superiority would simply be a comparison of how capable the opposing forces are, as he does not think there is any ability to maneuver in cyberspace.

I think Butler misses two points in his analysis. First, I think he is incorrect in his assertion that planners do not design campaigns to attain cyberspace superiority. The Georgian case study from 2008 is a prime example, the details of which are in chapter 5. Just as in the air domain, well-designed campaigns will plan to get enough cyberspace domain superiority to accomplish their overall objectives.

Secondly, superiority in the other domains is not a "shallow descriptor;" we can see that the relative strengths of the combatants do not directly determine who has domain superiority. The entity with the better-equipped, trained, and larger force does not always achieve land, maritime, or air superiority, why should cyberspace be any different? There is ample opportunity for an agile combatant to "maneuver" in cyberspace by creatively applying the cyberspace power he has against appropriate enemy weak points. While Butler and Libicki do not see much utility to cyberspace superiority, some authors see value to the concept without proposing a detailed theory of how to gain it.

Several authors support cyberspace superiority as a concept without providing a detailed map to gaining and maintaining it. Daniel Kuehl defines cyberspace superiority as, "the degree to which one can gain advantage from the use of cyberspace while if

[41] Butler, "Refocusing Cyber Warfare Thought," 52.

necessary preventing one's adversaries from gaining advantage from it."[42] This explanation is very close to the Air Force doctrinal definition and includes both offensive and defensive elements of cyberspace superiority.

Merna Hsu also supports cyberspace superiority as a concept when she states that, "…cyberspace superiority may be gained and maintained in a manner that exploits aspects significant to controlling the other mediums."[43] She is unfortunately vague about how a combatant can precisely gain and maintain cyberspace superiority.

Charles Eassa identifies cyberspace superiority as mirroring air and maritime superiorities although he does not think it is measurable and his proposed method of gaining it is too general to be helpful.[44] As for how to gain cyberspace superiority he says,

> To gain superiority, the CCDR [Combatant Commander] must have unfettered access in a constantly evolving and always contested environment. This requires a greater degree of integration of actions and capabilities and at lower echelons than ever before to achieve this effect. Actions at all levels focus on ensuring required information flows through the cyber domain while maintaining access or control of the infrastructure necessary to gain cyber superiority.[45]

"Unfettered access" sounds great, but Eassa tells you to achieve it by "integration of actions" and "maintaining access or control." It is hard to disagree, but these concepts are too broad and not actionable. "Maintaining access and control" is a way to define what cyberspace superiority is, but it does not tell you what to do to get it. Integration

---

[42] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem." in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, DC: Potomac Books, 2009), 37.
[43] Merna H., H. Hsu, "Gaining and Maintaining Cyberspace Superiority: Quest for a Holy Grail?" (Master's Thesis, The School of Advanced Air and Space Studies, 2009), 45.
[44] Charles N. Eassa, "Enabling Combatant Commander's Ability to Conduct Operations in the Cyber Domain" (Master's Thesis, U.S. Army War College, 2012), 14.
[45] Eassa, "Enabling Combatant Commander's Ability to Conduct Operations in the Cyber Domain," 15.

will be important to gaining cyberspace superiority but advocating "a greater degree of integration" without providing specific organizational recommendations is not useful. One author provides a more in depth view of how to achieve cyberspace superiority.

McCarthy provides a more comprehensive analysis of gaining and maintaining cyberspace superiority. He states that combatants seeking cyberspace superiority should focus on controlling the flow of traffic in the cyberspace domain to degrade the enemy's ability to use cyberspace.[46] He goes on to identify the control of chokepoints as the most efficient means of creating cyberspace superiority.[47] Here there is a solid concept that I will use to produce a more fully developed theory of how a combatant can gain cyberspace superiority. McCarthy came to this conclusion after studying domain control theory from maritime domain chokepoints where combatants could deny transit to enemy traffic while retaining it for friendly forces. If control of chokepoints were currently technically and politically feasible in cyberspace, this method would be the most efficient.

Unfortunately, at the current time, policy and technical limitations make controlling chokepoints in cyberspace challenging. The network design of cyberspace enables most traffic seamlessly and rapidly to divert around attempted blocks with no active intervention by the user. In addition, because of the problems with attribution, it will not be clear to a combatant that streams of information belong to the enemy. In addition, the enormous amount of data passing across chokepoints such as major undersea cables makes filtering it very difficult with current technology. Trying to filter

[46] McCarthy, "Traveling Domain Theory," 235-6.
[47] McCarthy, "Traveling Domain Theory," 288.

out enemy communications would likely slow friendly communication to a crawl, as the defender would need to inspect each packet to determine if he will allow it to pass or block it. The Chinese are the closest to being able to control traffic via chokepoints as they have limited portals into China and do not have any legal issues with intrusive scanning that would be illegal in most Western nations. Even so, they have great difficulty controlling information into and out of China. Despite our inability to copy the Chinese methods directly, there are other ways that Western nations can pursue cyberspace superiority.

Since controlling chokepoints is not practical with the current technology and structure of cyberspace, combatants should pursue whatever universal superiority is attainable, while focusing on the fight for local cyberspace superiority. In chapter 2, I built a generic model of domain control that was broken into offensive and defensive segments before I applied it to the land, maritime and air domains. Applying the same methodology to the cyberspace domain yields the model of gaining and utilizing cyberspace control in figure 8.

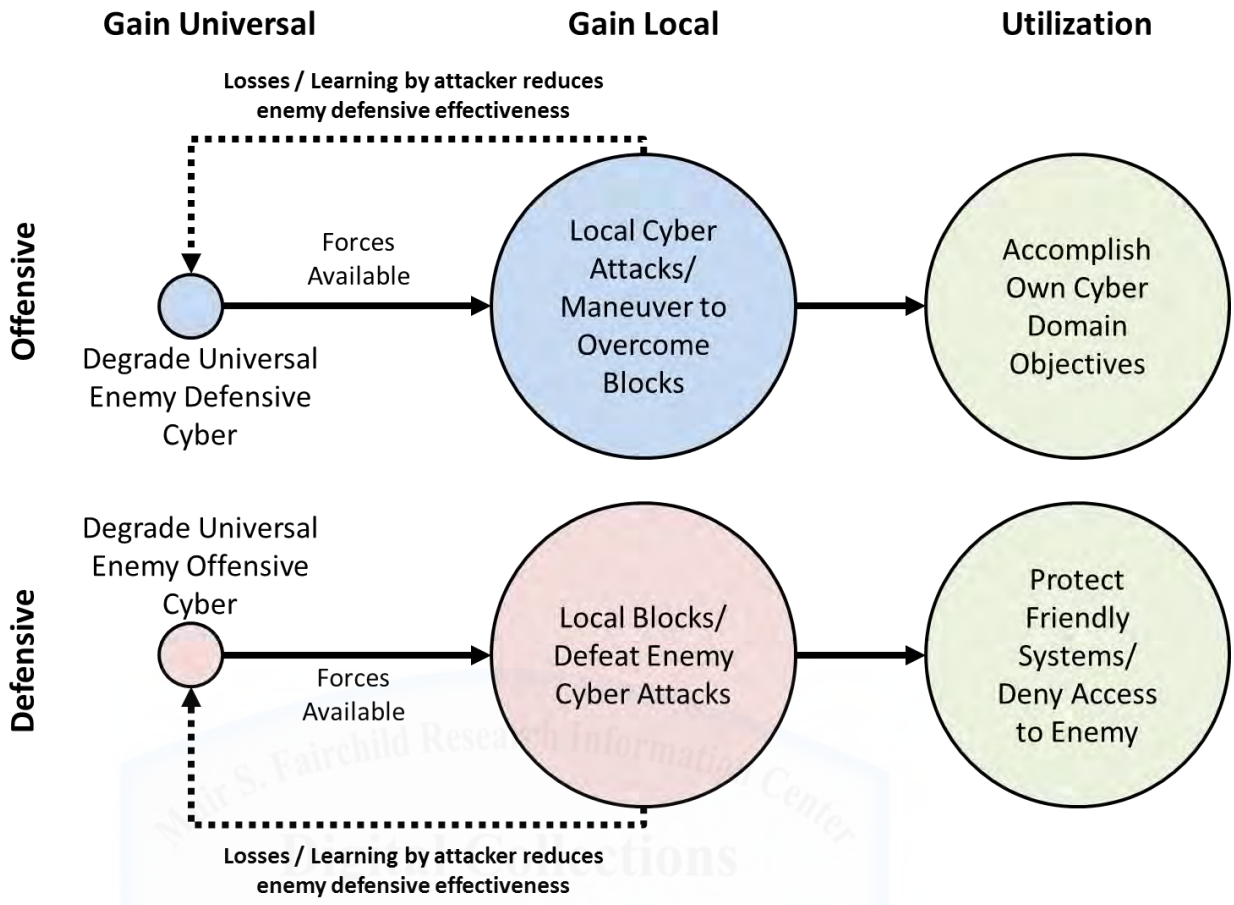

Figure 8 – Model of Gaining and Utilizing Cyberspace Superiority
Source: Author's Original Work

In cyberspace, the local level of superiority is far more important than the universal when compared to the other domains. First, it is difficult to move cyberspace weapons from one local area to another. Despite the fact that cyberspace weapons and tools are easy to copy, they do not transfer easily to other local areas. On the offensive side, the problem is that designers carefully tailor weapons to a precise target. Stuxnet, for example, would only function if it were on a system with one of two types of Siemens controllers, and only if the weapon detected a specific configuration of the controllers. On the defensive side, moving upgraded defenses from system to system is somewhat

easier, but still challenging because many systems are incompatible or run different operating systems. Many users and even IT professionals are slow to patch their systems, which slows the transfer of defensive upgrades to different local areas. For example, one month after an important Java security update, only 7% of users had downloaded the patch.[48]

Second, offensive and defensive forces in cyberspace are very different, which prevents combatants from moving between offensive and defensive missions. In contrast, the infantry, armor, and artillery of the land domain can all act on the offense or defense; the same is true of ships or multi-role fighter aircraft. In cyberspace, offensive weapons have no utility as defenses and vice versa. This limitation removes flexibility available in the other domains when combatants are moving forces and allocating them from the universal level to various local areas.

A third reason why combatants normally fight for cyberspace superiority at the local level is the highly specialized, single system characteristic of cyberspace weapons. Attackers have to design offensive weapons to attack a specific system. In the air domain, a 500-pound general-purpose bomb from an aircraft can destroy a bridge, tank, ship, or building. In the cyberspace domain, attackers have to design most offensive weapons for a specific system configured to work in definitive ways, with particular patches and connections. Designers have to create very specific weapons because they normally rely on vulnerabilities that are dissimilar in different systems. As a simple

[48] Dan Kaplan, "One month after recent Java update, 7 percent of users patched," *SC Magazine for IT Security Professionals*, 5 June 2013. http://www.scmagazine.com/one-month-after-recent-java-update-7-percent-of-users-patched/article/296431/.

example, a Windows virus sent to an Apple machine normally does nothing interesting at all because it is speaking the wrong language.

A final reason why cyberspace superiority tends to be local is that it is extremely difficult for combatants to find and attack enemy cyberspace "fleets" and "armies." Cyberspace weapons are more difficult to find than tanks, artillery, ships, and aircraft. The key resource in a cyberspace weapons system on offense or defense is the highly trained people, who are very hard to find and target. A combatant can hide a cyberspace lab or operations center in just about any non-descript building with no identifying smokestacks or cooling towers.

In addition, the relative unimportance of physical distance in cyberspace makes it very easy for cyberspace forces to disperse widely across multiple installations. Cyberspace operators do not have to be concentrated to be effective. Cyberspace defenses are broken into multiple systems and locations so even if an attacker takes down the systems in one local area, the rest are not directly affected. This fragmentation does not mean there may not be opportunities to degrade overall enemy cyberspace capability, but these opportunities will not be routine and will often require support from other domain forces.

Directly targeting cyberspace forces will generally require the utilization of physical domain forces as the most important cyberspace forces are in the physical domains. For example, if a cyberspace facility is located, a combatant could attack it directly with land, maritime, or air-based kinetic forces. The loss of the equipment, and more importantly personnel, could have a significant impact on the enemy's universal cyberspace superiority and could affect multiple local areas, as those resources are not

available. A bomb down an air conditioning duct is not the only possibility for degrading an enemy's cyberspace capability at the universal level, but it is one of the most straightforward.

While a combatant can probably not destroy the enemy's cyberspace weapons from cyberspace due to backups, an attacker could render the enemy's offensive weapons ineffective if he analyzed them before the enemy launches them. It is conceivable that a clever cyberspace attacker might be able to locate, or use a spy to access, an enemy's stock of cyberspace weapons. Even if the weapons themselves were untouched, if the attacker could determine what vulnerabilities they utilized and then patch those vulnerabilities, it would significantly degrade the enemy's offensive cyberspace potential. If the enemy has limited access to cyberspace, an attacker has another option.

In a fight with a nation having limited cyberspace portals, an attacker could take those portals down via cyberspace or physical attack. This approach would correlate well to McCarthy's suggested strategy of focusing on chokepoints. For example, if an attacker disrupted all three of China's portals to the Internet, it could reduce the number of attacks China could launch in return. However, taking down portals would not completely eliminate potential enemy attacks, as there will always be ways around disabled portals such as via satellite communications. It would also be very difficult to take down enough portals in a well-connected nation such as the United States to have much of an impact. The enemy will react to the down portals, but these attacks may still be worthwhile even if they only reduce his effectiveness slightly. In cyberspace, physical destruction such as a bomb onto an Internet portal will be the exception; much more common will be countering enemy cyberspace weapons through learning.

Cyberspace weapons can sometimes have physical effects, and non-cyberspace weapons from the other domains can create physical losses that affect cyberspace assets, but in the vast majority of cases, what causes a weapon or tool to lose its effectiveness in cyberspace is learning by the enemy. For cyberspace attackers, enemy learning is the principal threat, as once the enemy learns how the attack functions, the defenders can normally inoculate their systems against that particular attack as I discussed earlier. The weapon itself has not been touched, but it has lost its ability to produce effects, as the enemy system is now immune to its attacks.

Although their problem is less acute, cyberspace defenders face a similar dynamic. As an attacker probes a set of defenses and learns where the weak points and gaps are, the system's defenses become less effective. Stuxnet is an example where the creators of a weapon made adjustments based on learning to reach their objectives more effectively.[49] This learning is generally much faster for defenders than attackers, so offensive weapons lose their effectiveness much more quickly. These losses will generally have their most pronounced impact on the local instead of the universal level of cyberspace superiority.

The local level of cyberspace superiority is more important because of the very different offensive and defensive forces, the difficulty of attacking universal cyberspace forces, and the dispersed character of cyberspace resources. The method of gaining local cyberspace superiority will be quite different for the attacker and defender.

[49] Sanger, *Confront and Conceal*, 203.

An attacker will gain local cyberspace superiority by successfully accessing enemy systems to accomplish desired objectives. Doctrine has defined cyberspace superiority as the ability to conduct operations without prohibitive interference. Therefore, if an attacker is attaining his objectives in cyberspace, he is also gaining cyberspace superiority. Conflicts for cyberspace superiority are dynamic; the defender will attempt to stop the attacker at the same time of the attack.

A defender will gain local cyberspace superiority by successfully blocking the enemy from achieving his offensive objectives, and protecting friendly access to cyberspace systems. A defender's objectives in cyberspace are both negative and positive. On the negative side, the defender is attempting to prevent the attacker from accomplishing his objectives whether they are overt or covert. On the positive side, the defender is attempting to keep his or her friendly systems up and running effectively. Keeping friendly systems are up and running does not assume success for the defender. The attacker may not be trying to disable the defender's systems, but may have more subtle objectives. An attacker could be attempting to manipulate data inside a defender's systems to produce bad decisions by the defender's leadership. Just because the system appears to be functioning does not mean the defender has successfully maintained cyberspace superiority if the system has become secretly corrupted. Once a combatant gains local superiority, he can then utilize it to achieve his objectives through several mechanisms.

Use of Cyberspace Superiority

A combatant seeks various uses for superiority in the offensive and defensive realms of cyberspace. On the offensive side, an attacker will use superiority to accomplish his objectives. This use will normally be either through strategic information warfare or by providing support to other domain forces. On the defensive side, a defender will use cyberspace superiority to protect his systems and prevent the enemy from achieving his offensive objectives. Both the offensive and defensive sides of cyberspace are important to combatants; I will start the discussion with the offensive use that gets the most attention in the press, strategic information warfare.

Strategic Information Warfare

The first way that an attacker can utilize cyberspace superiority to deliver military power is through strategic information warfare.[50] Strategic information warfare is when an attacker attempts to achieve effects directly through cyberspace. Cyberspace superiority for an attacker is a prerequisite to effective strategic information warfare and is just as important for the defender who is trying to stop him.

An attacker must achieve local cyberspace superiority and overcome a system's defenses to accomplish strategic information warfare. For example, if an attacker wanted to shut down a power grid, he is first going to have to get through the defenses. Just overcoming enemy defenses is not sufficient to ensure a successful strategic information warfare attack. Cyberspace superiority is defined as the ability to accomplish friendly objectives through cyberspace so the attacks need to contribute to the attacker's

[50] For a more complete description of strategic information warfare and how it operates, see appendix C.

objectives. If an attacker's objective was to shut down enemy radar and he successfully disabled the power grid, but the radar remained functional on a backup generator, the attack was a failure despite its success at taking down the power grid. Cyberspace superiority is a pre-requisite to a successful strategic information warfare attack, but it is not sufficient, and the attack can still be unsuccessful at accomplishing an attacker's objectives. Cyberspace superiority is also important for defenders protecting their systems from strategic information warfare.

Defenders need cyberspace superiority to protect their systems from strategic information warfare. For a defender, this is generally accomplished by excluding attackers and mitigating the effects attackers have if they get into a system. This is normally accomplished via a large range of various defenses that are discussed in detail in appendix C. The method of gaining cyberspace superiority is very different for attackers and defenders in strategic information warfare, although cyberspace superiority is vitally important to both. While strategic information warfare gets most of the press attention, there are more important uses of cyberspace superiority.

Cyberspace as an Enabler of other Domain Forces

Cyberspace forces' most important contribution in current warfare is as an integrator and enabler of other domain forces. Unlike the land domain, cyberspace superiority does not matter on its own, what matters is what you can do with it. The most important thing that combatants can do with cyberspace superiority is enable success in the other domains.

One of the first things that cyberspace superiority brings to a combatant is the ability to integrate forces in the other domains to enable effective joint warfare. Most of

the modern joint communications and collaboration tools rely on cyberspace superiority to function. An army unit may speak directly to a pilot via a radio to coordinate the final stages of an airstrike in support of the ground unit, but everything that got the aircraft over that particular army unit relied upon communication and planning systems that require cyberspace superiority to function. The same holds true even within a single domain where, for example, naval combatants normally plan and coordinate via cyberspace based systems. If a combatant is part of a coalition, cyberspace enabled communications systems and planning tools are even more important. There are a multitude of other cyberspace driven tools that enable modern warfighters.

The physical domains do not rely on cyberspace only for integration, there are numerous cyberspace-enabled capabilities that modern combatants would be hard pressed to give up. In the land domain, friendly tracking systems, computerized logistics systems, data-links between vehicles and units, Unmanned Aerial Vehicles (UAVs), and many other enablers of modern warfare depend on cyberspace. Data links and network centric warfare connect naval combatants even more closely together via cyberspace support to the maritime domain. In the air domain, not only are aircraft and IADS tied together and controlled via cyberspace enabled command and control, the Joint Forces Air Component Commander (JFACC) builds and disseminates the Air Tasking Order (ATO) utilizing cyberspace assets. If a cyberspace enemy deprived U.S. forces of the cyberspace assets in their operations centers, U.S. forces would struggle to produce an ATO, and then would have limited means of disseminating it once they did. Given that the ATO is a crucial element of the execution of U.S. airpower, its loss would be a crippling blow to operations in the air domain. Cyberspace superiority can protect

friendly capability to move and communicate, but it can also reduce the enemy's ability to operate effectively.

Cyberspace superiority can enable success in the other domains by confusing and blinding enemy forces, whose vulnerability will depend on the extent to which they rely on cyberspace. Removing cyberspace enablers will have a much greater effect on a technologically dependent opponent such as the United States, and less impact on a less technologically dependent opponent such as North Korea. Even with a lower technology foe such as Iraq in 1991, a combatant can achieve important effects.

Analysts will likely never see support to other forces from cyberspace as decisive or "war winning," but it can certainly enable victory. At the extreme of success, an enemy can be like the Iraqi army of 1991, waiting in their positions, with no supplies, no coherent orders, and no idea where the enemy is or where the enemy is going. If someone blindfolds one of the two boxers in a fight, the blindfold may only be in a supporting instead of an operational role, but it certainly influences who wins. Cyberspace's supporting role to the other domains is the second mission set that a combatant can undertake with cyberspace superiority, the third is the defensive role of protecting friendly systems and preventing the enemy from accomplishing his objectives.

Protecting Friendly Systems

While it often receives less attention, protecting friendly systems and denying access to the enemy is likely the most important result of cyberspace superiority for a highly connected nation such as the United States. The more connected and cyberspace reliant a nation is, the more devastating it is if an attacker can disrupt those systems.

U.S. Forces have become increasingly reliant upon cyberspace-enabled tools and connectivity such as data links and friendly tracking systems. Connectivity can greatly increase effectiveness. For example, the installation of data link systems into fighter aircraft greatly increases their effectiveness. The down side is that pilots can become so dependent upon the new systems that they are unable to accomplish their missions if they are lost.[51] The same is true across other types of domain forces. Beyond degradation of fielded military forces, a nation's infrastructure can come under assault if cyberspace superiority is lost.

On the home front, the loss of cyberspace superiority will open up the nation's infrastructure to potential long-range attack. The electrical grid, water, transportation, and communications infrastructure are critical to modern life. Their loss would be far more important today than 100 years ago when much of the population still lived in rural settings and were either involved in, or at least close to food production. If an attacker could disrupt these systems, they could exert tremendous pressure on decision makers to concede issues not involving the survival of the nation. The amount of pressure that an attacker can bring to bear will vary depending on the targeted nation's level of dependency on cyberspace.

Taking down the electrical grid in North Korea is unlikely to cause them to surrender in a perceived fight for national survival; taking down the electrical grid in the United States may have a greater impact. The importance of the issues under discussion to the nation under attack is a critical variable. In Vietnam, the United States did not

[51] The impact is even greater when a new generation of personnel has never operated the system without data links. Older personnel may be able to adapt and utilize the system at a lower level of efficiency using old techniques not reliant upon data links; new personnel will have more difficulty.

suffer a military defeat, but the nation determined that the cost of continuing the war was not worth the potential gain. If the Chinese were invading the West coast while demanding unconditional surrender, it is unlikely that the United States would capitulate if the power grid went down. If the Chinese were demanding that the U.S. stay out of a fight over Taiwan, the response from U.S. decision makers to the loss of the power grid might be different. One of the key inputs into a decision maker's calculus will be how persistent they expect cyberspace effects to be.

Persistence of Cyberspace Superiority

The persistence of cyberspace superiority will generally be very short due to the replicability of cyberspace, its great speed of action, and the rapid degradation of offensive cyberspace weapons. The primacy of the local over the universal level in cyberspace superiority discussed earlier is also an important driver in cyberspace superiority's lack of persistence. The characteristic of cyberspace affecting persistence that is most unlike the other domains is its replicability.

Software and data in cyberspace are replicable, which makes software and data based attacks easier to recover from. One way for a defender to reduce the effects of an attack is if he keeps several complete up-to-date copies of software and data in locations inaccessible to an attacker. If an information system is "destroyed," and then is back up and running a few hours later from a clean backup copy; the window of effect from even a successful attack is very short. If a defender can copy the software and data of a system, he could easily repair damage done by non-hardware attacks.[52] The increasingly

[52] Libicki, *Conquest in Cyberspace*, 5.

inexpensive replicability of cyberspace systems also makes attacks based on manipulating data harder to execute. A defender can crosscheck multiple copies of information and see if an attacker has modified the data. This replicability of cyberspace contributes to the short timescale of most attacks because recovery tends to be very fast. In addition to its replicability, cyberspace's lack of distance also decreases persistence.

Physical distance is less important in cyberspace than in the other domains. According to journalist Robert O'Harrow, "It almost doesn't matter where hackers work. In the physics governing cyberspace, hackers, terrorists and cyberwarriors can operate virtually next door…"[53] Push a button in Istanbul and a power grid in Connecticut goes down; cyberspace warriors do not have to gain physical access or even be on the same continent as the target. Where physical distance and location still matter is if an attacker is going to use the other domains to attack cyberspace assets such as with an air delivered bomb on the enemy cyber operations center. The lack of virtual distance in cyberspace also contributes to its great speed of action, which reduces the persistence of cyberspace superiority.

The short timescales of cyberspace produce great speed of action and rapidly changing dominance. Robert Belk and Matthew Noyes state that the millisecond timescale of cyberspace communications makes cyberspace warfare more rapid than any of the other domains.[54] The release of a single weapon in cyberspace that travels to its target and has catastrophic effects in seconds can change the entire battlespace. This speed, and lack of distance, means that a battle, or even a campaign, can turn in an instant

[53] Robert O'Harrow, *Zero Day: The Threat in Cyberspace* (New York: Diversion Books, 2013), Kindle Location 135, part 1.
[54] Belk and Noyes, "On the Use of Offensive Cyber Capabilities," 16.

from success to failure and back again. Another characteristic of cyberspace discussed earlier that affects persistence is the importance of the local over the universal level.

The greater importance of local versus universal cyberspace superiority reduces persistence significantly. If a combatant achieves a high level of universal superiority in a domain, it can be hard for the enemy to recover, as he has to build up an entirely new set of forces to contest domain superiority again. Thus, if combatants fight for domain superiority at the universal level, as has often been the case in the maritime domain, superiority can be very stable. If, as in cyberspace, the domain superiority achieved is only local, then the enemy does not have to build new forces, he only has to shift them from another local area and he can rapidly contest domain superiority again. As has been discussed, cyberspace tools may not shift easily from one local area to another if they are different systems, but combatants can move the people writing the tools effectively and quickly.

Another reason why cyberspace superiority will not tend to be persistent is the rapid degradation in the effectiveness of offensive cyberspace weapons once defenders discover them. Defenders can easily access the hardware and software on their systems and can normally eliminate the weapons quickly once discovered. If the weapon is too hard to eliminate in a system, administrators can erase and completely reload systems from clean backup copies. In the attacks on ARAMCO, or the 2011 and 2013 North Korean attacks on South Korea, administrators were able to clean the systems and get them back running in days once the attacks started and the weapons could no longer hide. Cyberspace weapons are akin to glass swords: they can be very sharp and lethal, but they

tend to break on the first swing. Because offensive cyberspace weapons lose their effectiveness so quickly, attackers can normally use them only once.

Once a defender finds an enemy weapon, he will be able to inoculate his other systems and the weapon will lose most of its utility for future attacks. The following medical analogy is apt.[55] A vaccine protects the body by "teaching" the immune system what to look for. In the same way, once an administrator teaches an anti-virus system what to look for, that anti-virus system will be very effective at keeping out a particular attack. As a result, cyberspace weapons tend to be single use. In other domains, weapons can keep their relative effectiveness after an attacker has used them, but not so in cyberspace. Designers of cyberspace weapons can use several approaches to mitigate this rapid loss of effectiveness.

One approach is to co-opt the defender's tools. North Korea used this concept when they utilized the update mechanism of a popular South Korean anti-virus program to propagate their 2013 attack.[56] However, taking over the anti-virus program did not produce long-term cyberspace superiority as one can see in the case studies.

A second tactic is to propagate widely an aggressive weapon so that it can re-infect machines that defenders clear; it appears that Stuxnet used this strategy.[57] This approach was part of the success of Stuxnet and attackers could use aggressive infection protocols for other cyberspace weapons. The drawback to this approach is that the more aggressive the weapon is, the more likely it is to trigger alarms, even though it is

[55] Paul Rosenzweig suggests that the medical world presents a very useful template for looking at cyberspace. Rosenzweig, *Cyber Warfare*, Kindle Location 752, chap. 34.
[56] Economist. "North Korean cyber-rattling." *The Economist*, 17 May 2013. http://www.economist.com/blogs/babbage/2013/05/digital-warfare.
[57] Shakarian, et al., *Introduction to Cyber-Warfare*, Kindle Location 7003, chap. 13.

attempting to stay hidden. It appears that the aggressive nature of the upgraded Stuxnet is what caused it to get out "in the wild."[58]

A third approach by cyberspace attackers is to produce different versions of the weapon that are just different enough to escape notice by anti-virus programs relying on signatures of previous versions. Defenders who look for signatures that are similar, but not the same as known threats, can mitigate this technique.

A fourth method is to focus on chokepoints and expensive, difficult to replace infrastructure components. Attacking software will not yield much effect if the defender can reload from clean copies. Destroying racks full of servers will also not accomplish much if the enemy has warehouses full of replacements or an easy way to route information around the disabled node. However, there are hardware components that are more expensive and difficult to replace than generic routers and computers. Some of these targets may not be cyberspace components at all, but instead support the cyberspace components such as power generation. For significant, persistent effects, cyberspace attackers should look to attack difficult to replace hardware in support of a chokepoint that carries multiple communication pathways.

A final approach to achieve longer persistence of cyberspace superiority is for the weapon to stay hidden and work in the background. Defenders can only reconstitute damaged systems and inoculate against attacks they know have occurred. Certain types

[58] For more information, see the Stuxnet section of the case studies. In short, it appears that Stuxnet got out in the wild when an Iranian scientist inadvertently interrupted the more aggressive version of Stuxnet in the middle of a process. The scientist then plugged an infected computer into the Internet and despite not being on the right system Stuxnet had already completed the protocols to check for a specific system and started to propagate. This circumstance resulted in it spreading beyond the nuclear system the designers intended to infect. Sanger, *Confront and Conceal*, 204.

of attacks lend themselves to this technique. If an attacker is attempting to manipulate databases, collect information, or create physical effects that look like they have another source, the weapon can stay hidden. Stuxnet and various espionage attempts are examples of this sort of attack.

These strategies can help extend cyberspace superiority, but the examples of nation-state cyberspace attacks currently known show a short duration for cyberspace superiority. In the eight cases studied in chapter 5, seven of them persisted less than a week and the one case that lasted longer was because Stuxnet was able to hide successfully its activity from the Iranian defenders for an extended period of time. In some cases, such as ARAMCO and Stuxnet, defenders brought in outside resources, which are available to any nation-state. A broad exception to the short-lived characteristic of attacks is espionage; I excluded them from the case studies for reasons I discuss in chapter 5. If an attacker is able to stay hidden, the attack can continue, but this tactic is only possible if there is no external manifestation of the attack detected by the defender. To be able to analyze properly the persistence of cyberspace superiority in the case studies, it will first be necessary to develop a measurement system capable of measuring the level of cyberspace superiority in a given conflict.

Measurement Concepts of Cyberspace Superiority

Measuring cyberspace superiority will be challenging due to the characteristics of the domain. The anonymity and secrecy that surrounds cyberspace operations makes it difficult to determine what is actually going on in any given conflict. This uncertainty can even include who the combatants are, as attacking nations may attempt to cast the

blame on someone else. Comparing force capabilities in cyberspace is also very challenging, which limits the utility of order of battle comparisons as a measurement tool. Finally, developing a numerically based cyberspace superiority measurement system will at some point require quantifying qualitative data, which is often a difficult and error prone process. Fortunately, there are elements of domain superiority from the other domains that we can utilize.

In the land domain, analysts measure superiority by whose soldiers are in possession of the terrain and who has the acquiescence or support of the population. These metrics have limited utility to cyberspace superiority other than the general principle that superiority is a relative measurement based on a dyad in conflict, not an absolute measurement. Measuring superiority in the maritime domain is more applicable to cyberspace.

In the maritime domain, analysts measure universal superiority by the strength of the opposing fleets, and local superiority by who is able effectively to utilize sea lines of communication. While comparing cyberspace "fleets" is not a promising approach, the parallels between moving goods on the seas and moving information in cyberspace implies utility to measuring the health of lines of communication in cyberspace. For cyberspace combatants, this utility will most often be on the defensive side and will involve effectively measuring the health of defended cyberspace systems. Analysts should couple this measurement of the functionality of defensive systems gleaned from the maritime domain with offensive measurement from the air domain.

Measuring air domain superiority principally revolves around measuring combatant's ability to achieve their objectives in the air. This concept has direct

applicability to cyberspace where two of the principal measurements will be the accomplishment of objectives by cyberspace attackers, and the prevention of the completion of enemy objectives by cyberspace defenders. These measurement concepts will lie at the heart of cyberspace superiority measurement.

Cyberspace domain superiority is fundamentally about a combatant being able to achieve his objectives in cyberspace while preventing the enemy from achieving his, thus objectives will be key to measurement. A cyberspace superiority measurement method should account for both the offensive and defensive sides of a conflict. It also must include measurement of the success of both combatants, as superiority is a relative measurement. We need to develop a method that allows for the incorporation of multiple measurement factors into a single system.

A weighted preference measurement construct will provide the analytical rigor and flexibility needed for cyberspace superiority measurement. I will develop the details to this approach in chapter 4. The measurement system will provide the ability to combine multiple inputs and weight them for their relative importance. Before turning to the detailed measurement system in the next chapter, I will review what we have determined so far about cyberspace superiority.

Conclusion

Cyberspace is a unique domain with distinctive characteristics, many of which have a significant impact on cyberspace superiority. It is a man-made domain that an analyst can usefully model by Libicki's linguistic model. Utilizing Libicki's three layers of the physical, syntactic, and semantic is helpful as cyberspace superiority operates very

differently in each category. In the physical layer, the fight is over the hardware of cyberspace, whether via bombs from the air domain or cyberspace weapons that attack hardware components. The syntactic layer is composed of software and it is here that worms, Trojans, and viruses operate in an attempt to manipulate the instructions and rules of cyberspace systems. Finally, it is at the semantic level that one stores information in cyberspace; this level is the arena of information operations and changing enemy decision making via manipulation of data and information. Cyberspace superiority operates on all of these layers in different ways; however, cyberspace superiority first requires access.

Contesting cyberspace superiority has a low cost of entry, but significant capability will still require a substantial investment. While a laptop and an Internet connection are very cheap, developing modern and effective cyberspace weapons such as Stuxnet or Flame is not. The low cost of entry means there are many more players in the struggle for cyberspace superiority than is the case in the air or maritime domains where the cost of entry is high. There are not only nation states, but also private individuals and collectives such as Anonymous or "patriotic hackers" that can weigh in and influence cyberspace superiority; for example, in conflicts between nation states such as the conflicts between Russia and Georgia or Estonia where Russian "patriotic hackers" played a major role. These hackers had some initial advantage over their opponents as the offense currently has the advantage in cyberspace.

The offense has the advantage in cyberspace, as it is the attacker who remains hidden, while the defender is visible and vulnerable. This is the opposite of the land domain, where attacking soldiers generally have to move out in the open while defenders can remain hidden until they choose to engage. This circumstance provides an initial

advantage to the offense over the defense in cyberspace superiority. This advantage will normally play out at the local instead of the universal level of cyberspace superiority.

While universal cyberspace superiority is theoretically possible, in the majority of cases, superiority will be determined at the local level. The local level of cyberspace superiority is usually predominant in part because designers tailor cyberspace weapons to both the local area and the system within which they designed them to operate. This specialization makes it much harder for a combatant to shift resources from one local area to another and decreases the importance of universal cyberspace superiority. The differences between offensive and defensive weapons in cyberspace further intensify the relative importance of the local level.

Another factor that drives the importance of local superiority is the inability of combatants to target the enemy's cyberspace "fleets" and "armies." On the universal level, cyberspace superiority assets are very easy to hide and extremely difficult to target and destroy. When the opportunity presents itself, a combatant should target any universal cyberspace targets, such as a cyberspace operations center, that present themselves. However, combatants should expect these opportunities to be rare. Once a combatant has gained superiority, he can utilize it for several purposes.

Combatants can utilize cyberspace superiority principally in three ways, to pursue strategic information warfare, to support other domain forces, or to protect friendly systems. Most combatants will attempt to do all three to some degree during a conflict. Strategic information warfare is where a combatant attempts to achieve some effect directly through cyberspace. Strategic information warfare is similar to strategic bombing in the air domain, both in the misuse of the word "strategic" and in the desire to

achieve direct effects. Shutting down an enemy power grid would be an example of strategic information warfare and strategic information warfare gets the majority of the press about cyberspace warfare.

However, at the current time cyberspace is actually more important as an integrator and enabler of other domain forces. A modern cyberspace dependent force like the U.S. military can be extremely effective when everything is working, but also effectively hamstrung by an opponent who successfully attacks their cyberspace systems.

Finally, any combatant with cyberspace infrastructure will want to defend his or her systems to prevent the enemy from achieving his objectives. The rapid degradation of cyberspace attacks once launched significantly helps the defender.

Once an attacker is unmasked, physical ownership, replicability, and the frangibility of offensive weapons will enable defenders to recover rapidly and thus the persistence of cyberspace superiority will be very short. While attackers have an initial advantage, this advantage rapidly deteriorates once the defender realizes he or she is under attack. Historically, defenders have been able to rebuild their systems very quickly by either restoring from backups or rebuilding systems. Some defenders, such as the less capable Saudis and Georgians, brought in help in order to defend their cyberspace systems. These factors have resulted in a very short persistence for cyberspace superiority.

The best way for an attacker to maintain greater persistence of cyberspace superiority is through remaining masked and hidden, which is a tactic only available in certain situations. Stuxnet took this approach by masking its effects to make the Iranians think the failures of their systems were due to manufacturing errors or poor design. As a

result, Stuxnet was able to maintain cyberspace superiority much longer than has been observed with other cyberspace weapons. If an attacker is attempting to completely collapse the enemy's power grid, it is unlikely that the defender will not notice what is going on. To properly analyze the persistence of cyberspace superiority, we need to develop a measurement tool.

By utilizing a weighted preference model, cyberspace combatants can usefully determine what level of cyberspace superiority they have achieved versus an opponent. The critical inputs into the measurement system are the objectives of the attacker and his level of success as well as the importance of various systems to the defender and his level of success in defending them. This information is difficult to obtain, but a weighted preference model will still allow for analysis.

The unique characteristics of the cyberspace domain produce three major elements of cyberspace superiority. First, offensive and defensive tools in cyberspace operate differently, with the offense having an initial, but short-lived advantage. Second, local cyberspace superiority will be far more important than universal cyberspace superiority, which will normally be unachievable and not worth pursuing. Third, cyberspace superiority will normally not be very persistent, as the initial advantage for the offender will evaporate quickly once the defender realizes he or she is under attack. Combining the characteristics discussed previously with the domain superiority components from chapter 2 gives the following table.

Table 2 – Summary of Domain Superiority Characteristics

Geography and Characteristics	
Land	Physical terrain such as mountains, rivers, and swamps dictate lines of communication and which forces are most effective

	where • Combat tends to be sequential with forces excluding each other from areas of their control while protecting their own lines of communication
Maritime	• Maneuver space is bounded by land masses and ports which form chokepoints • Sea lines of communication are the key element worth fighting over • Accessed via expensive technology (ships) and expensive entry points (ports)
Air	• Open and relatively unbounded without natural chokepoints • No clear front line--involves civilians directly in combat operations • Characterized by great speed of action • Dependent upon technology for access • Accessed via expensive technology (aircraft) and expensive entry points (airfields) • Dominance in this domain is not sufficient for victory, however it enables the land and maritime domains
Cyberspace	• Manmade but connected to the physical world • Can usefully be modeled by Libicki's three layers of physical, syntactic, and semantic • An entry-level capability for a nation-state in cyberspace can be very economical; however, significant capability is still expensive • The network structure of cyberspace gives it a high level of built-in resiliency to attacks that focus on interfering with communication between nodes • There are chokepoints in cyberspace that we can consider as roughly analogous to mountain ranges or other features in the land domain • There are two facets to cyberspace's changing geography over time, the first is that combatants can connect, disconnect, or change the linkages between the components that create cyberspace • The second facet of cyberspace's changing geography is that designers continue rapidly to make the individual hardware more capable • Because of the small number of military cyberspace forces in relation to the vast amount of civilian cyberspace, normally no nation state will have superiority in most areas of cyberspace • Combatants may restrain themselves in cyberspace to avoid crossing perceived global norms of cyberspace as a global

	common • Offensive cyberspace weapons have no ability to "see" and react to each other, thus there is no analog to a meeting engagement in cyberspace
Offensive or Defensive Primacy	
Land	• With modern weapons the defensive has primacy as the defender can stay under cover while the offender must unmask to advance
Maritime	• There is no clear offensive or defensive primacy in the maritime domain o Normally both offensive and defensive forces can see each other at the same distance o Exceptions include submarine warfare which favors the offender and a fleet in a defended port which favors the defense
Air	• Older theorists favored offensive, but the advantage has shifted back and forth over time depending on technology
Cyberspace	• The advantage in the cyberspace domain goes to the attacker who can be proactive as he can remain hidden and anonymous, while the defender is out in the open and reactive
Method of Gaining Superiority	
Land	• Universal – Defeat enemy army to allow physical access to the terrain and then gain control and support of the population • Local – Defeat local regular or insurgent forces
Maritime	• Universal – Defeat enemy fleet or blockade them in port; weaker combatant can contest by keeping a "fleet in being" and executing small counter attacks • Local – Disrupt enemy shipping while protecting your own
Air	• Offensive universal – Degrade enemy strategic IADS • Defensive universal – Degrade enemy offensive airpower • Offensive local – Defeat enemy local IADS • Defensive Local – Defeat enemy local offensive airpower
Cyberspace	• Controlling chokepoints is one way of establishing universal cyberspace superiority, however it will normally not be possible • There are a number of reasons why local cyberspace superiority will normally be all that is achievable o It is difficult to move cyberspace weapons from one local area to another o Offensive and defensive forces in cyberspace are very different and are not interchangeable o The specialization of cyberspace weapons that attackers design for a single system o It is extremely difficult for combatants to find and attack

	enemy cyberspace “fleets” and “armies” • An attacker will gain local cyberspace superiority by successfully accessing enemy systems to accomplish desired objectives • A defender will gain local cyberspace superiority by successfully blocking the enemy from achieving his offensive objectives, and protecting friendly access to cyberspace systems
Use of Superiority	
Land	• Often control of the land domain will terminate the conflict; if not, combatant can extract resources for continued combat in other areas and domains
Maritime	• Enable shipment of military and commercial goods • Project power into the land domain while preventing the enemy from doing the same
Air	• Offensive – Directly striking enemy centers of gravity to either affect enemy capabilities or change enemy decisions; Support other domain forces • Defensive – Prevent enemy from striking friendly centers of gravity
Cyberspace	• There are three principal methods for combatants to utilize cyberspace superiority o Strategic information warfare: creating direct effects through cyberspace o Enabling and integrating other domain forces: utilizing cyberspace to increase the effectiveness of land, maritime, air, and space domain forces o Protecting friendly systems: maintaining the effectiveness of friendly cyberspace systems
Persistence	
Land	• Land domain superiority tends to be persistent due to greater influence of the universal level of superiority as well as the sequential tendencies of land combat, the inertia of populations whose support changes slowly, and the current primacy of the defensive
Maritime	• Whether the maritime superiority gained is local or universal will greatly affect the persistence of maritime superiority o If a combatant can achieve universal maritime superiority through defeating the enemy fleet, then persistence can be high o If the enemy refuses to fight a major fleet action for universal control, then control will not only be localized, but also fleeting as the enemy can dash out of port to raid convoys and establish local control in an area, but then retreat back into port when threatened by the main adversary fleet

Air	Because of the high mobility of air domain forces to move from one local area to another, a combatant will be able to achieve persistence of superiority in the air domain only if he is able to achieve universal versus local air superiority
Cyberspace	The persistence of cyberspace superiority will generally be very short due to the replicability of cyberspace, its great speed of action, and the rapid degradation of offensive cyberspace weapons once defenders discover them
Measurement Concept	
Land	Whose soldiers are in possession of the terrain Metrics to determine the level of support of the population
Maritime	Universal – Remaining capability of enemy fleet Local – Metrics to measure friendly and enemy utilization of sea lines of communication; Ability to project power into other domains
Air	Ability to achieve objectives in the air Relative measurement and trends of resources
Cyberspace	On the offensive side, key inputs of cyberspace superiority include the offenders objectives and level of success On the defensive side, key inputs of cyberspace superiority include the level of functionality of defended systems and their importance

Now that we have gathered both the elements of domain control from the other domains in chapter 2 as well as the unique characteristics of the cyberspace domain as they apply to cyberspace superiority, we can move forward to create the weighted preference measurement system.

4 – MEASURING CYBERSPACE SUPERIORITY

Thus far, we have explored the elements of domain superiority and applied them to cyberspace superiority; before moving onto the case studies, we need a method of measuring cyberspace superiority. When we examined measurement concepts of cyberspace superiority in chapter 3, we saw that the two most significant components of a cyberspace superiority measurement system should be the combatant's objectives in cyberspace and their ability to defend their systems. As we will have to balance several factors, we need to utilize a methodology that weights multiple factors.

While there are challenges with measuring cyberspace superiority, a weighted preference analytical model can provide powerful instrument that will provide a methodology to minimize the challenges of a sparse and qualitatively based data set. Quantifying the qualitative inputs is an important element that I discuss more fully in appendix A and the model allows the incorporation of multiple inputs from whatever relevant sources are available in a particular case. I use this model to focus measurements on areas of greatest importance to characterize cyberspace superiority and to analyze the case studies.

The cyberspace superiority measurement system I will develop here will balance the offensive and defensive sides of cyberspace superiority while accounting for the varying levels of reliance upon cyberspace in different nations. On the offensive side, I will consider an attacker's success against cyberspace objectives with the importance of those objectives to determine a level of offensive cyberspace superiority. On the defensive side, I will utilize the defender's success in maintaining the functionality of

defended systems and include the importance of those systems to the defender to measure defensive cyberspace superiority. I will round out the model with a variable to account for the different reliance upon cyberspace in different nations. Before building the cyberspace superiority measurement model, I will first look at a few of the challenges to building a successful measurement system in cyberspace.

Challenges of Cyberspace Superiority Measurement

Measuring cyberspace superiority is difficult for several reasons, starting with the difficulty of getting accurate information on a cyberspace conflict. Any measurement system can only be accurate if an analyst can feed correct information into the system. In cyberspace, that information is often difficult to obtain due to classification issues, attribution uncertainty, and structural incentives on all sides to falsify data. Cyberspace combatants classify their capabilities and efforts at high levels to protect them. Most cyberspace attackers cloak their activities in cyberspace and rarely admit to attacks so provide no information on how effective they thought they were. Depending on their objectives, defenders may also choose either to deliberately exaggerate, or downplay the scale and impact of a particular attack. Even if an analyst can find good information, converting qualitative data into quantitative inputs remains a concern.

Quantification and coding of the data is a major issue with developing a cyberspace superiority measurement system. If a targeted system is "partially disrupted," does that represent 20% capability or 80% capability? If one does not code the inputs into the system in a systematic and repeatable manner, then the outputs lose analytical significance, no matter how elegant the measurement system. Accordingly, I developed

coding methodology for the major inputs into the system and detail this method in appendix A. For the measurement system to be useful for analysis, different researchers should decide on similar inputs given the same data set and coding rules. With a method of quantifying the inputs in appendix A, we can start developing the measurement system by examining the definition of cyberspace superiority.

Elements of the Definition of Cyberspace Superiority needed for Measurement

The definition of cyberspace superiority given in AFDD 3-12 is, "The operational advantage in, through, and from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference."[1] Pulling this definition apart yields several crucial phrases that help build the structure of the measurement tool.

The first key phrase of the definition is "operational advantage." The first definition of operation in JP 1-02 is, "A series of tactical actions with a common purpose or unifying theme."[2] Cyberspace superiority is about more than measuring the success of aggregated tactical actions. If those actions are not moving a combatant any closer to their objectives, then they are not relevant. Objectives are the way an attacker will normally spell out the desired common purposes or unifying themes that he or she is seeking in cyberspace and those objectives must be a key component of any measurement system. The word "advantage" in the definition once again illustrates that cyberspace superiority is relative, as advantage has no meaning without having an advantage in relation to something or someone else.

[1] AFDD 3-12, *Cyberspace Operations. Change 1*, 2.
[2] Department of Defense, *Joint Publication 1-02*, 15 December 2012, 216.

The second key phrase of the definition is "to conduct operations." Cyberspace superiority is not meaningful unless it allows you to do something. This phrase also gives the key to measuring cyberspace superiority. Any measurement system should reflect a clear connection between how easily a combatant can conduct operations, as that is what cyberspace superiority allows you to do, quite literally by definition. Note that operations do not have to be offensive. Feeding the troops can be "conducting operations" just as much as sending out a patrol. A measurement of cyberspace superiority will need to account for both the offensive and defensive components.

The third key phrase of the definition is "given time." Cyberspace superiority will be limited temporally. As the level of cyberspace superiority will change with time, it also follows that the advantage can, and will, swing back and forth between combatants. A measurement of cyberspace superiority may be just a snapshot in time, not a final answer.

The fourth key element of the definition is that cyberspace superiority takes place in a "given domain." The language here is somewhat unfortunate as what the U.S. Air Force meant by a "given domain" is not the whole of the cyberspace domain. Instead, they are referring to a given domain as a smaller sub-set, or slice, of cyberspace that is of particular interest to a combatant. This meaning is clear from the next sentence in AFDD 3-12, which states that cyberspace superiority can be localized. Just because a combatant has superiority in one slice of cyberspace, it does not follow that they will be dominant across all of cyberspace. This fragmentation means that cyberspace superiority is highly localized and the measurement system must account for multiple levels of superiority across different slices, or systems, in cyberspace.

The final key concept in the definition for developing a method of measurement is that an attacker needs to accomplish all of the elements mentioned "without prohibitive interference." This statement again highlights the relational aspect of cyberspace superiority. As one combatant is attacking enemy systems, the enemy is generally not just defending his systems; he is actively attacking the first combatant's systems, who is trying to overcome the second combatant's defenses, etc. This dynamic is the heart of the wrestling analogy used by Clausewitz and we must keep it in mind while developing the measurement scheme.[3] I will start by considering the easiest possible case of measurement.

Measurement in the Trivial Case

To illustrate the measurement system that developed for this project, consider first a "trivial case" where there are only two actors, combatant A and combatant B, only one system in cyberspace, and a single attack from A to B to accomplish a simple objective that is either completely met, or completely fails. In this case cyberspace superiority would be a binary measurement, if combatant A is successful, A's cyberspace superiority would be 1.00. If the attack were unsuccessful or blocked, then A's cyberspace superiority would be 0.00. The next step is to examine how to measure objectives in warfare when they are not simple binary measurements.

Measurement of Objectives as an Input to Measuring Cyberspace Superiority

Since the level of success an attacker has in achieving objectives in cyberspace is a key element of cyberspace superiority, it will be necessary to look at how to measure

[3] Clausewitz, *On War*, 75.

success against objectives in general. Fortunately, Joint Forces Command (JFCOM) has done a great deal of work already in this area. JFCOM developed one of the more detailed systems shown in figure 9.

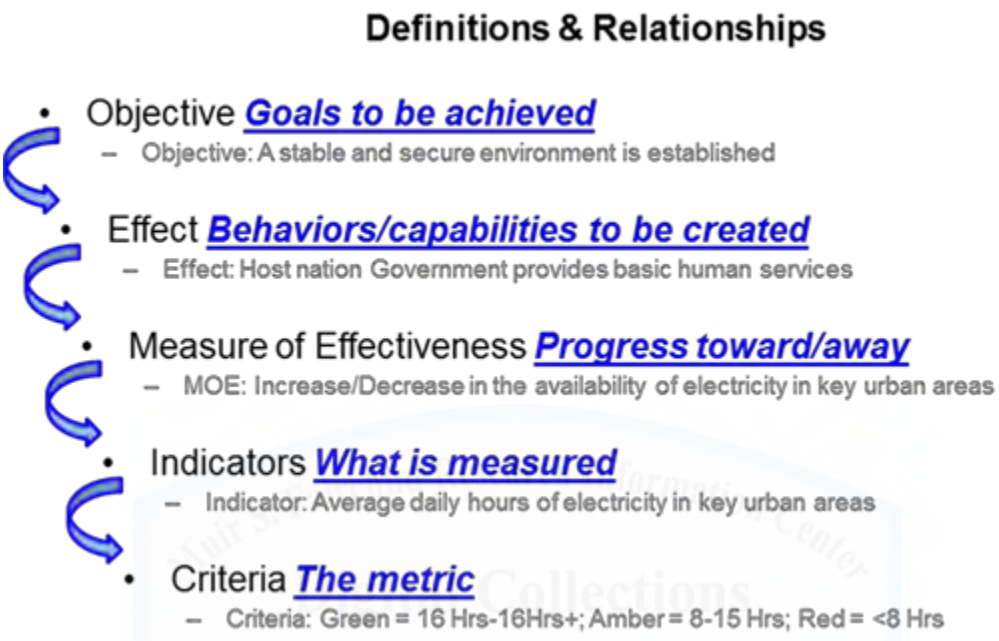

Figure 9 – Effects Component Summary
Source: Adapted from Figure I-3, U.S. Department of Defense, U.S. Joint Forces Command. "Joint, Techniques, and Procedures: Assessment of Joint Operations." 10 March 2008, I-6.

The lower levels in figure 14 feed into the higher levels and it is important to note that there can be multiple indicators for each Measure of Effectiveness (MOE), multiple MOEs for each effect, and multiple effects for each objective. Depending on the situation, there can also be only one effect per objective, etc.

As an example of how this method of measurement can work in a physical domain, an attacker's objective might be to reduce enemy logistical capability. The effect would be that an attacker has immobilized enemy armored forces due to a lack of

supply. The corresponding MOE could be an increase/decrease in the supply status of enemy armored divisions. An indicator would be the level of supply possessed by specific divisions in the regular categories of supply. For example, the defender's metric might be that for a specific adversary division, green is 24 hours or less of fuel reserves, amber is 24-72 hours, and red is more than 72 hours of fuel reserves.

If in the previous example an attacker sought the same objective through the cyberspace domain, then nothing changes in the measurement. The tools would change from kinetic forces to cyberspace forces but the objective of reducing enemy logistical activity, the effect desired, the MOE's and metrics could be similar or the same. When measuring the success of a combatant in achieving his or her objectives, it is not the medium or domain, but the effects that matter. Planners already understand this system of objective measurement across the Department of Defense (DoD), and operators use similar systems today in USAF Combined Air Operations Centers (CAOCs) to measure success. A system of measuring success against objectives is only the first step and helps develop one of the inputs for measuring offensive cyberspace superiority.

Measuring Offensive Cyberspace Superiority

On the offensive side, the first independent variable is S, the level of success an attacker has achieved against a particular cyberspace objective. S can range from 1.0 if an attacker has completely met their objective to 0.0 if the attacker has not met any part of his objective. You can then utilize the effects, MOEs, indicators, and criteria to determine an S for each objective. For example, if one of the commander's objectives was to shut down an enemy power grid to put pressure on enemy decision makers, the

effect might be that the enemy's power control system was non-functional. The measures of effectiveness might include how well the control system was running the power grid. An indicator would be whether the enemy was providing power to the population. The criteria might be what amount of the enemy's population still had effective power. S would come out of the calculation as a percentage, for example, if the enemy power grid was providing 50% of its normal power, then S = 0.50.

An attacker needs to calculate S for each objective and then multiply it by a weighting factor W. The weighting factor captures the level of importance that the commander has assigned to each objective and all the weighting factors have to add up to 1. For example, if there were three objectives and the commander assigned 50% weight to the first one, 30% to the second and 20% to the third, then W_1=0.5, W_2=0.3 and W_3=0.2.

Once the success levels and weighting factors have been determined, the overall Offensive Cyberspace Superiority Index (OCSI) can be determined by summing up the multiples of all the objectives and their weights.

$$OCSI = \sum_{1}^{n}((S_1 \times W_1) + (S_2 \times W_2) + (S_3 \times W_3) + \cdots (S_n \times W_n))$$

or

$$OCSI = \sum_{k=1}^{n} S_k \times W_k$$

OCSI will range from 0.0 to 1.0 with 1.0 equaling complete offensive dominance and 0.0 representing total failure in the offensive arena.

Measuring Defensive Cyberspace Superiority

The critical factor in measuring your defensive cyberspace superiority is the level of functionality (L) in critical systems. This measurement L is the defensive equivalent of S and I express it from 0.0 to 1.0 like S. If a system was considered 50% functional, then L = 0.50.

Next, L is multiplied by C, which is a measure of the system's criticality. C, like W, must add up to 1.0 so if the first system was considered twice as important as the second and third systems then $C_1 = 0.50$, $C_2 = 0.25$ and $C_3 = 0.25$.

This construct yields a measurement similar to OSCI but on the defensive side named Defensive Cyberspace Superiority Index (DCSI). Like OSCI, DCSI will range from 0.0 to 1.0 and I calculate it via the following formula:

$$DCSI = \sum_{1}^{n}((L_1 \times C_1) + (L_2 \times C_2) + (L_3 \times C_3) + \cdots (L_n \times C_n))$$

or

$$DCSI = \sum_{k=1}^{n} L_k \times C_k$$

Note that the critical systems are only those in the local area that combatants are contesting. Recall that in cyberspace superiority, the local level is the one that has the greatest impact and the one we focus on in these calculations.

In some cases, such as Russia's attack on Estonia, there is only one attacker and one defender. Since Estonia was not attacking Russia at all, the Estonian OCSI would be 0.0. In addition, since the only critical systems included in DCSI are those in a contested local area, the Russian DCSI was 0.00.

Reliance on Cyberspace

Before I can combine the offensive and defensive indices into the overall local Cyberspace Superiority Index (CSI), I need to address another issue. Not every nation is equally dependent upon the cyberspace domain. For example, in a conflict of the United States versus North Korea, North Korea would happily eliminate cyberspace capability for everyone. The elimination of the cyberspace domain would significantly increase North Korea's combat power relative to the US because North Korea does not rely on cyberspace as much as the United States does to generate combat power. To account for this factor, I have utilized an independent variable R in the calculation, which accounts for how reliant a nation is on its cyberspace systems. There will be two Rs, one for each combatant in the pair and the value of the two Rs has to add up to 1.0. For example if nation A and B were equally reliant upon cyberspace, then $R_A = 0.50$ and $R_B = 0.50$. However, in a pairing like the United States and North Korea where there is a significant disparity, $R_{\text{United States}}$ might equal 0.95 and $R_{\text{North Korea}}$ might equal 0.05.

A high level of reliance on cyberspace does not automatically imply a high level of vulnerability to cyberspace attack; in fact, the more important cyberspace is to a nation, the harder it will work to defend it. I will capture this factor in the lower levels of success that attackers will have against more effectively defended targets and the greater resources required to affect the same percentage of assets. For example, a moderate amount of resources might be sufficient to disable 50% of the telecommunications infrastructure in a small underdeveloped nation. However, disabling 50% of the U.S. telecommunications infrastructure would require an immense expenditure of resources

and overcoming significant cyberspace defenses. Now we are ready to put the defensive and offensive sides together.

Cyberspace Superiority Index

The Cyberspace Superiority Index (CSI) combines a nation's offensive and defensive success while accounting for varying levels of cyberspace importance for different combatants. It is imperative to capture the importance of the cyberspace domain to each combatant because complete dominance of an area that is of little importance to the enemy is less valuable than dominance of an area upon which he is reliant. This element also acts as a multiplier to ensure that the final CSI is between 0.0 and 1.0, despite adding the two indices together. I calculate Nation A's CSI by:

$$CSI_A = \left((OCSI_A \times R_B) + (DCSI_A \times R_A)\right)$$

Notice that I multiplied the offensive index by the defender's reliance on the cyberspace domain while I multiplied the defensive index by the offender's reliance. This cross multiplication is because the importance of success in the offensive domain depends on how reliant the defender is on cyberspace, while the importance of success at achieving cyberspace superiority in the defensive domain also depends on how reliant the defender is on cyberspace. To return to the North Korean example, the U.S. establishing high offensive cyberspace superiority is less important than North Korea establishing high offensive cyberspace superiority and R accounts for that fact. I calculate the CSI for nation B the same way:

$$CSI_B = \left((OCSI_B \times R_A) + (DCSI_B \times R_B)\right)$$

Relative Cyberspace Superiority Index

The final dependent variable is the Relative Cyberspace Superiority Index (RCSI), which is a measurement of which side has superiority. I calculate it per nation and simply determine it by:

$$RCSI_A = CSI_A - CSI_B$$

Since CSI_A and CSI_B range from 0.0 to 1.0, $RCSI_A$ can range from -1.0 to +1.0. At -1.0, nation B completely dominates A and at +1.0, nation A dominates nation B. Nation B's RCSI is the opposite and I calculate it by:

$$RCSI_B = CSI_B - CSI_A$$

If you substitute in the equations for OCSI and DCSI, you get the complete equation of:

$$RCSI_A = \left(\left(\left[\sum_{k=1}^{n} S_k \times W_k\right]_A \times R_B\right) + \left(\left[\sum_{k=1}^{n} L_k \times C_k\right]_A \times R_A\right)\right) - \left(\left(\left[\sum_{k=1}^{n} S_k \times W_k\right]_B \times R_A\right) + \left(\left[\sum_{k=1}^{n} L_k \times C_k\right]_B \times R_B\right)\right)$$

Initial Testing of the Cyberspace Superiority Index

To perform an initial test on whether RCSI provides a useful measurement of cyberspace superiority, I tested a number of simple hypothetical cases. I started at an extreme where combatant A had complete command of cyberspace. Nation A met all of their cyberspace offensive objectives and all of their cyberspace critical systems were 100% operational. Conversely, combatant B had achieved none of their cyberspace

objectives and none of their systems was functional. This scenario gave the following inputs and outputs:

$OCSI_A$= 1.00
$DCSI_A$= 1.00
R_A= 0.50
$OCSI_B$= 0.00
$DCSI_B$= 0.00
R_B= 0.50

CSI_A= 1.00 and CSI_B= 0.00, which yields:

$RCSI_A$= 1.00
$RCSI_B$= -1.00

As expected, combatant A has complete "command of the cyberspace" with an RCSI of 1.0 while combatant B is achieving nothing in the cyberspace domain with an RCSI of -1.0.

At the middle, if the sides have equivalent capabilities then:

$OCSI_A$= 0.50
$DCSI_A$= 0.50
R_A= 0.50
$OCSI_B$= 0.50
$DCSI_B$= 0.50
R_B= 0.50

CSI_A= 0.50 and CSI_B= 0.50, which yields:

$RCSI_A$= 0.00
$RCSI_B$= 0.00

Neither side has cyberspace superiority. Both A's and B's efforts exactly balance each other out and give an RCSI of 0.0 to each. However, if side A gains an advantage then:

$OCSI_A$= 0.75
$DCSI_A$= 0.50
R_A= 0.50

$OCSI_B$= 0.50
$DCSI_B$= 0.25
R_B= 0.50

CSI_A= 0.63 and CSI_B= 0.38, which yields:

$RCSI_A$= 0.25
$RCSI_B$= -0.25

Note that as the importance of the cyberspace domain for side B diminishes, A's relative advantage shrinks as well.

$OCSI_A$= 0.75
$DCSI_A$= 0.50
R_A= 0.75
$OCSI_B$= 0.50
$DCSI_B$= 0.25
R_B= 0.25

CSI_A= 0.56 and CSI_B= 0.44, which yields:

$RCSI_A$= 0.13
$RCSI_B$= -0.13

The importance of the reliance factor can also be seen in a case where each side is equally successful at offense but unsuccessful at defense. If the reliance factor is balanced then you get:

$OCSI_A$= 0.75
$DCSI_A$= 0.25
R_A= 0.50
$OCSI_B$= 0.75
$DCSI_B$= 0.25
R_B= 0.50

CSI_A= 0.50 and CSI_B= 0.50, which yields:

$RCSI_A$= 0.00
$RCSI_B$= 0.00

Each side has the same RCSI as you would expect. However, if the cyberspace domain is more important for combatant A than combatant B, then you no longer have parity:

$OCSI_A = 0.75$
$DCSI_A = 0.25$
$R_A = 0.75$
$OCSI_B = 0.75$
$DCSI_B = 0.25$
$R_B = 0.25$

$CSI_A = 0.38$ and $CSI_B = 0.63$, which yields:

$RCSI_A = -0.25$
$RCSI_B = 0.25$

This example might occur if a high technology nation is fighting one that does not utilize information systems as much to generate combat power. These results suggest that the weighted preference methodology is sound and this approach should yield a useful measurement of cyberspace superiority for a given moment if the inputs are correct. The model also has some other uses.

Other Applications of the Measurement Tool

In addition measuring cyberspace superiority, this weighted preference analytical model has potential utility for training. Combatants could utilize this measurement system in training exercises. Instructors could incorporate this measurement concept into computerized scoring systems to project the trainee's effectiveness.

Another area where combatants could utilize this measurement system is in planning for cyberspace operations. This measurement system could provide a method to quantify the expected success of various courses of action to improve planning. This system will also provide the ability to look at tradeoffs within courses of action. This

measurement system will provide an analytical framework that planners can use to examine branches and sequels to their plans. Wishful thinking as an input will still result in bad output, but a more rigorous analytical approach can be helpful.

This measurement methodology also has tremendous potential for combatants to utilize in cyberspace domain wargaming as a scoring mechanism. It could provide a clear quantitative index of how each side is doing in an exercise versus a purely qualitative approach. If trainers or simulators are used, referees could build this scoring mechanism into the wargaming system. If a combatant ran the same scenario multiple times with different cyberspace domain units, it could help identify best practices as well as encourage higher levels of performance as each unit attempted to beat the "high score." Like any measurement system, this one can be "gamed" once the participants understand the weighting of the factors. Referees will have to ensure that the wargaming stays grounded in valid intelligence and commander's expectations on the importance of various objectives. Overall, this system provides a flexible tool that can be adapted to various scenarios and situations.

Conclusion

Combatants in cyberspace can utilize the weighted preference analytical model presented here to analyze which of two combatants has superiority in cyberspace. The model also quantifies the amount of cyberspace superiority for a combatant at a given time and in a local area. Combatants can use the measurement system for planning, wargaming, and training, and it balances both offensive and defensive achievement in cyberspace.

The weighted preference measurement system developed in this chapter includes both the offensive and defensive elements for both combatants. The measurement system starts by defining an attacker's objectives and then weighting those objectives. It balances the measurement of success on the offensive for both combatants with their level of success in defending their systems weighted towards the systems that are more critical to each combatant. Finally, I incorporate a variable to allow for the varying levels of reliance that different nation-states have on cyberspace. This system also needs valid inputs.

While the measurement system here is methodologically solid, it is dependent upon accurate inputs, which may be difficult to obtain. There are three major issues with inputs. First, cyberspace combatants often obscure everything they do in cyberspace conflict behind walls of anonymity and high levels of classification. Second, cyberspace combatants on the offense or defense often have numerous incentives, not just to hide, but also to actively mislead and lie about the outcomes of a cyberspace conflict. Finally, analysts must translate fundamentally qualitative data into quantitative inputs. Analysts mitigate the first two issues by seeking as much data from as broad a set of sources as possible. Analysts can alleviate the third issue with a detailed coding system.

Analysts need to code inputs into the measurement system in a repeatable manner such that different analysts would give similar inputs from the same data. To accomplish this repeatable coding, I provide a detailed breakdown and definitions of the various inputs in appendix A. I will use this coding methodology in the next chapter to analyze the cyberspace superiority case studies.

5 – CYBERSPACE SUPERIORITY CASE STUDIES

While it would certainly be preferable to have a large number of case studies with detailed information on cyberspace operations and their effects, such cases and data does not exist, as the conflicts have not happened yet. To draw an analogy from airpower, cyberspace today is in a similar place to where airpower was before World War I. Before World War I, a few nations in conflicts, such as the Italians in Ethiopia, had taken airplanes to war, but they had not yet been very effective. Cyberspace warfare today is in an analogous position, as nations have made cyberspace attacks in support of national objectives, but there have been no worldwide cyberspace wars and attackers have barely scratched the surface of the potential of cyberspace conflict. This lack of historical record does not mean it is not worth trying to figure out how cyberspace superiority could work in a future conflict. We can look at the evidence available and extrapolate concepts from warfare in other domains as was done in chapter 2. One of the issues with the cyberspace evidence is the difficulty in finding out what happened in the few case studies available.

During a conflict, a combatant will have some idea of his or her progress towards their objectives based on Battle Damage Assessment (BDA) and intelligence work, but there will always be uncertainty because the enemy will be actively trying to deceive and mislead. The attacks that you think have been so successful may have been diverted into "honey nets" and the Integrated Air Defense System (IADS) you thought your cyberspace warriors took down is actually completely operational and just waiting for

your aircraft to get within range before the enemy turns it back on.[1] Even absent active attempts by an enemy to mislead, other structural issues will make accurate data elusive.

After a conflict has terminated it will normally be hard to acquire appropriate data to determine who achieved what level of cyberspace superiority during a conflict for several reasons. Most information related to the specifics of attacks and defense in cyberspace is highly classified. Even if a researcher has full access to the classified information on one side, it is unlikely that they would have access to the classified information on the other side. Actually, the situation is worse than that because most cyberspace information is not only classified, it is so highly compartmentalized so that not only does the left hand frequently not know what the right hand is doing, often the left hand does not know the right hand exists. According to the Vice Chairman of the Joint Chiefs of Staff, General Cartwright, "We make sure the recce teams don't tell the defenders what they found, or the attacker, and the attackers go out and attack and don't tell anybody they did. It's a complete secret to everybody in the loop and it's dysfunctional."[2] This problem is much more challenging for the analyst who is working at the unclassified level where information is abundant, but generally of low quality.

There is a fair amount of data out in the unclassified realm, but it is mostly of journalistic versus analytical in character. A researcher has to sort through the data available to establish the objectives of the attacker and what level of success an attacker

[1] "Honey nets" are networks that defenders use to feed attackers false information. More details on these defenses are in appendix C.
[2] General James E. Cartwright, USMC, comments at Air Force Association Air Warfare Symposium, February 8, 2007, reported in Franklin D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework." in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, DC: Potomac Books, 2009), 14.

achieved. In many cases, the identity of the attacker is even in doubt because most attackers, so far, have chosen to claim innocence. This uncertainty does not mean that it is impossible to analyze superiority in the cyberspace domain, but there will always be a level of uncertainty about the calculation of superiority in any particular case. Often, as in the case of Stuxnet or the Aramco attack, there is consensus in the open source press as to who did it and why, but there will not be certainty. Accordingly, it will be important to cast the net as broadly as possible to ensure that outlying data will not too easily skew the results of this study.

While I attempted to capture as wide a range of cases as possible, the struggle for cyberspace superiority under examination here is the one between nation states. As a result, the possible range of case studies is limited despite the multiple types of groups operating in the cyberspace domain.

Cyberspace Superiority Actors

There are four main types of actors in cyberspace. The first is what I term "cyberspace vandals"; these are the same people who used to spray paint the front of rival schools with scatological references, but they now can do it through cyberspace. Often, this attacker really is the stereotypical bored teenager with a computer in their parents' basement, in accordance with popular culture's idea of a hacker. Generally, this group has low skills and resources and relies on pre-packaged attack programs downloaded off the Internet. These scripts are the origin of the derogatory term "script kiddies" and this category of hacker is normally not a serious threat in cyberspace. The next three groups,

hacktivists, cyberspace criminals, and state actors are more serious threats, as they possess the capability to create their own attack and spyware programs.[3]

As you move up the cyberspace threat ladder, analysts refer to the second group as "hacktivists." These actors focus on a political end and can have significant capabilities although their skills range widely. There are large multi-national groups such as Anonymous as well as smaller more focused groups such as LulzSec. These groups generally intend to make some political statement, often about privacy, free speech, and governmental control of the Internet; however, their chosen causes are almost as numerous as the hacktivists themselves. These groups can have significant capability and cause difficulty for governments, but they are not part of the struggle between nation states and legal experts do not consider attacks by them as part of interstate warfare. The line between hacktivists and states can be blurred by so-called "patriotic hackers" when civilian activists are utilized by a government in pursuit of national ends. Examples of these types of attacks include the cyberspace attacks into Estonia in 2007 and Georgia in 2008. I will examine those attacks under the assumption that the attackers executed them were, if not under the direction of, at least in coordination with a state government. I will discuss the details of the evidence tying those attacks to the Russian government in the appropriate cases. The next threat group in cyberspace presents a more focused threat than typical hacktivists.

The third group active in cyberspace consists of professional criminals. They use many of the same tactics as state actors and can have significant capability. However,

[3] Alexander Gostev, "The Flame" Questions and Answers," *Securelist*, 28 May 2012. http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers.

their objectives are profit based and they are principally interested in making money. The easiest way to determine a state cyberspace attack from one undertaken by criminals is by examining the subject and characteristics of the attack. States can and do attack banking institutions in rival states, but they are usually trying to disrupt the banks, not steal money. Examples of these types of attacks include attacks on South Korean banks alleged to originate in North Korea and attacks on U.S. banks linked to Iran. A state actor is more likely to undertake a denial of service type of attack on a bank, as there is no theft, only disruption of the rival. A criminal organization is more interested in getting into the bank accounts and getting money out, or they rely on Internet fraud and spam e-mail. State actors can utilize criminal organizations just like hacktivists, and in one example, analysts traced many of the attacks on Georgia to the Russian Business Network (RBN), which was a Russian criminal organization.[4] I consider an attack to be state sponsored if a state was directing or coordinating an attack undertaken by criminal hackers in pursuit of state objectives. If criminal organizations are not reliable or capable enough, a state can also use its own military or governmental forces directly in cyberspace.

The final category consists of state actors, and the capabilities here range widely. Some nations have nascent cyberspace warfare programs and many are starting to build capable programs, but significant capability requires substantial expenditure of resources. While the cost of entry into cyberspace is low, a capable program requires more "means." Currently, the most capable nations in cyberspace include Israel, the United States, the

[4] Kenneth Corbin, "Lessons From the Russia-Georgia Cyberwar," *Internet News*, 12 March 2009. http://www.internetnews.com/govern-ment/article.php/3810011/Lessons-From-the-Russia-Georgia-Cyberwar.htm.

United Kingdom, China, and Russia.[5] It is difficult to establish an exact hierarchy since combatants do not openly display and discuss cyberspace assets. Other nations known to have cyberspace warfare programs that politicians often accuse them of using include North Korea and Iran. This project focuses on cyberspace conflict between state actors; however, other issues make it difficult to select cases to study cyberspace superiority.

One of the most common types of cyberspace attacks between state actors attempts to steal information. These attacks are, in principle, similar to sending in a "James Bond" spy with a fancy car and watch, but they are lower risk, as there are no operatives to compromise or expose. These attacks are important and can generate an operational advantage from cyberspace, but by their design, they are very hard to pin down. States engaging in cyberspace espionage do not publicize what they are doing, and victims rarely publish it unless they are trying for court convictions or to cast some blame on the attacker. If the attacker does his job correctly, the victim will never know the attack took place. Consequently, it is not a useful category to examine, as any case study that we know about was a failure on some level because we know about it.

Other types of cyberspace attacks produce obvious results, and in some cases overt effects are the point of an attack, such as the Georgian attacks where official government websites were replaced by images comparing the Georgian president to Hitler.[6] Unfortunately for analysts, it is often difficult to figure out the source of even an overt cyberspace attack.

---

[5] Stuart Fox, "Why Cyberwar is Unlikely," *Tech News Daily*, 2 July 2011. http://www.technewsdaily.com/6962-cyberwar-unlikely-deterrence-cyber-war.html.
[6] John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times*, 12 August 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0.

Nations often attempt to mask their actions in cyberspace; however, attribution is important, as understanding the attacker's objectives is a critical input into measuring cyberspace superiority. In the cyberspace world, it is extremely difficult to prove who was behind an attack even if it is widely believed that a particular country was responsible.[7] For this study, I will identify the presumed attacker as the one most often cited as behind an attack. This attribution may be incorrect in a specific case. For example, it is possible, though not likely, that the Russian government really had no part in the cyberspace attacks on Estonia and Georgia. Complete proof is not required to proceed on the assumption that the Russian government was involved, as this study is not a criminal court. Even if I turn out to be incorrect in one case, it will not necessarily invalidate all of my conclusions.

Another difficulty in examining cyberspace superiority case studies is the narrow evidentiary base. There are a few unclassified studies available on specific cyberspace incidents such as the US Cyber Consequences Unit study on the Georgian conflict or Jeffrey Carr's "Gray Goose" project; however, most sources are narrow in focus and journalistic instead of analytical in character. The information is available, but an analyst has to sift it carefully.

Most nations involved in a conflict in cyberspace have significant incentive to be less than fully forthcoming about their activities. Attackers often claim innocence or that someone is trying to frame them. China resolutely maintains that it is a victim in cyberspace, not a perpetrator of cyberspace espionage and attacks, despite significant

[7] Barrett, et al., "Assured Access to the Global Commons," 41.

evidence to the contrary.[8] Defenders have incentives to deceive or misdirect as well. If an attack was successful, but the defender does not want anyone to know, there can be a significant incentive to lie. The Iranians have steadfastly maintained that Stuxnet was not significant and was caught and stopped before doing substantial damage. Most non-Iranian sources have suggested otherwise. Sometimes a defender even has incentive to maximize the apparent damage in an attempt to cast additional blame on the attacker. Given the sources available, there will always be some doubt and great care is called for when examining the data.

Case Study Methodology

I selected cases to examine for the study that met two major criteria.[9] First, both sides in the conflict had to be, or were widely suspected to be, nation states. Second, the attacks had to have enough documentation in open source literature to allow me to examine them in sufficient detail to utilize the cyberspace superiority measurement tool to determine who achieved how much cyberspace superiority. The main elements of information included a reasonable level of confidence in the attacker's objectives, as well as the success of the attack and some information on the defender's actions.

[8] Even at the unclassified level, the Mandiant report provides substantial evidence that ties most Chinese origin attacks to a particular Chinese army unit, PLA Unit 61398. The report even provides pictures of the building that the Mandiant analysts believe is the source of these attacks. Across Western sources, no-one seems to take the Chinese denials very seriously. David E. Sanger, David Barboza and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S." *New York Times*, 19 February 2013. http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all&_r=2&.

[9] I excluded cases such as the Hezbollah, Hamas, and Palestinian attacks on Israel as there was only one nation state in the conflict. Granted that Hezbollah, Hamas, or the Palestinian Authority have some of the characteristics of nation states, but there is no evidence directly tying those organizations to the attacks on Israel. The attackers appeared to be "self-organizing" individuals outraged at Israel, rather than organized elements of a campaign undertaken by a central authority in pursuit of clear objectives.

An example of a case that I was unable to use was the alleged Iranian attack against U.S. banks in September of 2012. Unfortunately, there is nothing except suspicion to pin the attack on Iran and there is not enough information in the open press on what Iranian objectives were, or more importantly, what impact the attacks had. After a few banks discussed the attacks, the banks stopped talking to the press, leaving no way to determine what level of success the attacks actually had. Fortunately, there were enough cases left to investigate.

Once I had chosen a case study, I then analyzed whatever literature was available to determine the inputs into the cyberspace superiority measurement model. This normally involved searching first for analytical information, and then falling back on journalistic articles when required. The objectives of the attacker were the first input.

For a cyberspace attacker, their objectives, and the weighting of those objectives, are the key inputs. Examining the objectives of cyberspace attackers is not the purpose of these case studies. However, examining the attacker's objectives is necessary to develop the inputs into the cyberspace superiority model. The next step after determining the objectives and their weighting was to accomplish a similar analysis on the defensive side.

For a cyberspace defender, the level of functionality of their systems and how important those systems were to the defender are the key inputs. Like the objectives, this data is not the point of the case studies, but is necessary to understand who has how much cyberspace superiority during a conflict, so I can use the cyberspace superiority model.

Once I had input the data into the cyberspace superiority model, I could calculate the overall level of cyberspace superiority via the measurement system developed in chapter 4. This method allows an analysis to connect the specifics of the case to the level

of superiority gained by the combatants and the development of connections between elements that have an impact on cyberspace superiority. To help visualize the connections in a specific case study, I have developed an illustration of cyberspace conflict.

To show what tools are active in a particular case, I also provide a simple illustration of conflict in cyberspace and the tools most often used. In cyberspace conflict, combatants are attempting to connect their offensive means with their intended ways while defenders are attempting to interfere with both an attacker's means and ways. The attacker is attempting to interfere with the defender's blocks which sets up the contest for cyberspace superiority I illustrate in figure 10.

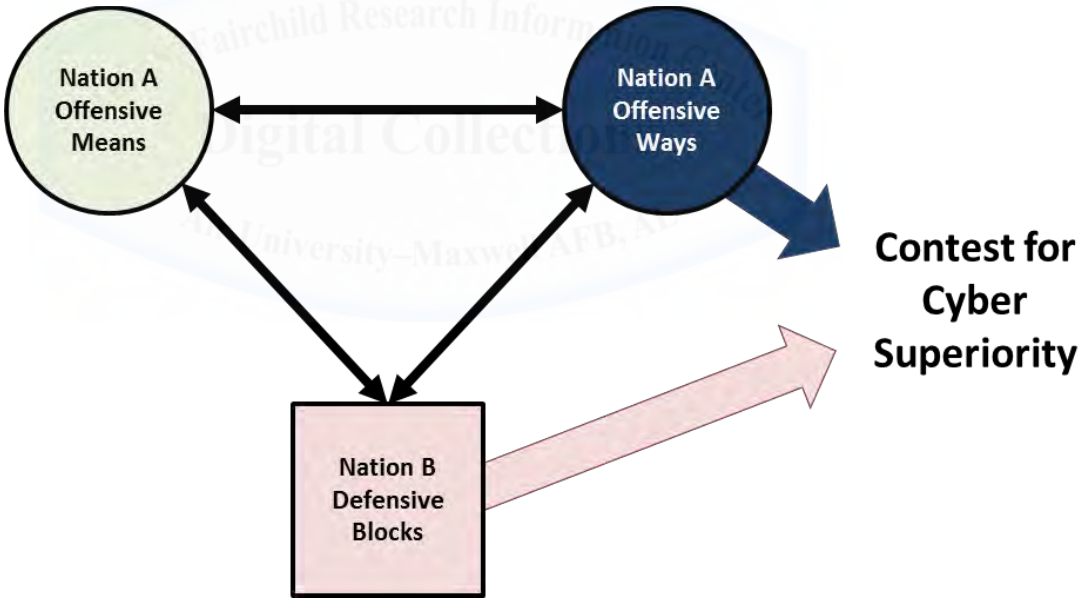

Figure 10 – Cyberspace Conflict
Source: Author's Original Work

This simplistic illustration can be useful when the actual means, ways, and blocks are included as a way to provide a sketch of who has superiority and what elements are operative in a case.

When the tools are included, I depict an illustration of the cyberspace conflict system in figure 11.

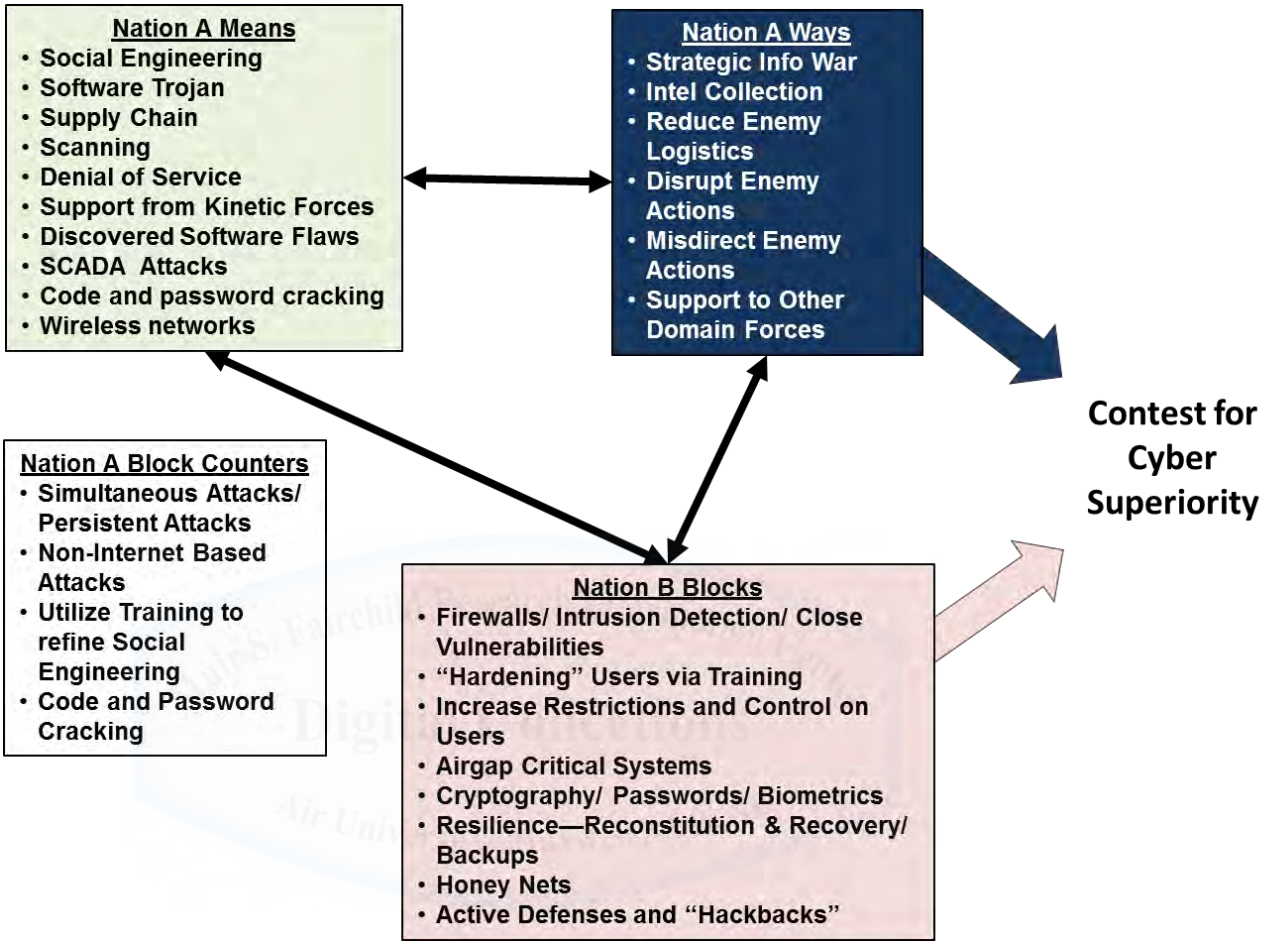

Figure 11 – Detailed Cyberspace Conflict Diagram with Tools and Ways
Source: Author's Original Work

A description of all these cyberspace means, ways, blocks and counter-blocks is included in appendix C. Note that the attacker aims some of his tools at mitigating or disrupting the defender's attempts to stop him, instead of directly at achieving cyberspace objectives. In each case in this chapter, I will provide a diagram with the elements combatants either did not use, or were unsuccessful with, in gray. This illustration will

provide an analyst with a broad overview of the operative elements before examining the details in the text.

To analyze how cyberspace superiority has worked in practice, I have selected three cases to examine in more detail. I selected the Russian attack on Georgia due to the depth of the sources coupled with the fact that it is the only case of cyberspace used in support of a conventional attack with clear attribution. I also selected the Stuxnet attack due to the depth of sources along with the fact that many commentators have seen it as a major turning point as the first attack known to have directly generated physical effects outside of cyberspace. The final case study that I selected for in depth analysis was the attack on Aramco where the attacker, presumably Iran, attempted to produce similar physical effects through a cyberspace attack but failed. In addition to the three case studies I develop in this chapter, I also examined five other cases. The detailed breakdown of the calculations for those five cases is in appendix B. The first case study I will examine in detail was the Russian assault on Georgia.

Russia versus Georgia 2008

The Russian and Georgian conflict of 2008 is one of the first cases of cyberspace superiority having an effect on conventional military operations. On 7 August 2008, a five-day war started between Georgia and Russia over two breakaway provinces, South Ossetia and Abkhazia. The war started with a Georgian attack into a breakaway region within its borders to re-establish government control, which led to a massive Russian

invasion and eventually to a EU brokered cease-fire.[10] What analysts did not fully appreciate at the time was that this incident was also the first documented case of a cyberspace warfare campaign used by an attacker in support of a conventional ground attack. The first cyberspace attacks were actually by the Georgians who started hacking South Ossetian media sites earlier in the week before the Georgian attack into South Ossetia.[11] What the Georgians apparently did not expect was the massive cyberspace assault that came right as Russian troops invaded not only the breakaway provinces, but also Georgia itself. To analyze the cyberspace superiority achieved by the combatants and its effects, we need first to examine each side's attacks.

Offensive Level of Success (S) and Weighting Factor (W) in Russia vs. Georgia 2008

The first step in determining an offender's objectives is to determine who the attacker was. In this case, the Russian government has never admitted that it was behind the wave of attacks; however, there is good reason to attribute the attacks on Georgia to them anyway.

It appears that "patriotic hackers" under the direction of Russian authorities executed the attacks in support of Russian forces. The identity of the attackers is significant as their objectives are an important input into the cyberspace superiority model. There are two clear indicators that the Russian government was behind the attacks. First is the timing of the attacks which started precisely in concert with the Russian military operation. Second, the precision of the attacks indicated that the

[10] British Broadcasting Corporation, "Russia in Georgia separatist pact." *BBC*, 17 September 2008, http://news.bbc.co.uk/2/hi/europe/7620972.stm.
[11] The Georgian military was goaded into attacking South Ossetia by attacks on Georgian villages, which gave the Russians the pretext they were looking for to invade Georgia. Shakarian, et al., *Introduction to Cyber-Warfare*, Kindle Location 940, chap. 3.

attackers had already done extensive reconnaissance and prepared for the attacks beforehand. These attacks were not something that a group of hackers created in response to unfolding events, the preparatory work had already been done.[12] As we start to develop a picture of what the Russians were seeking in cyberspace, we can also look at some of the things that they could have done, but chose not to, as clues.

Russian hackers did show a level of restraint and, "refrained from carrying out the sorts of attacks that would have done lasting physical damage to the Georgian critical infrastructure."[13] This restraint helps to frame potential Russian objectives leading to cyberspace superiority. Russia and Georgia have close and enduring economic ties and it appears that Russia sought immediate effect without causing lasting damage.

The two principal weapons used by the Russian hackers were denial of service attacks and discovered software flaws. For the software attacks, the Russians used Structured Query Language (SQL) injection attacks that enabled them to deface Georgian government web sites.[14] The Russians used these weapons to seek a number of apparent objectives. The first and most important objective appears to have been to disrupt enemy actions by attacking Georgian communications, both to reduce enemy information access, and to disrupt Georgian actions, as it was difficult for Georgian forces to know what was going on.[15] This disruption also made it difficult to supply Georgian forces, although the short scale of this conflict makes it difficult to analyze the effect the communications

[12] United States Cyber Consequences Unit, "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008," US-CCU Special Report, August 2009, 3.
[13] United States Cyber Consequences Unit, "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008," 5.
[14] Shakarian, et al., *Introduction to Cyber-Warfare*, Kindle Location 1043, chap 3.
[15] Rosenzweig, *Cyber Warfare*, Kindle Location 752, chap. 34.

attacks had on Georgian logistics. In any case, the communications disruptions also aided Russian ground and air forces that were attacking Georgian forces. In addition to these objectives supporting their forces, the Russians also utilized their cyberspace superiority to pursue strategic information warfare.

Some of the Russian's offensive objectives required the use of strategic information warfare.[16] Russia directly attacked Georgia's pipeline infrastructure through cyberspace. As argued by the United States Cyber Consequences Unit (US CCU), it actually appears that Russia may have been more interested in Georgia's oil and gas pipelines than protecting ethnic Russian civilians.[17] The first areas Russian forces seized were not civilian areas but Georgian ports and facilities for handling oil and gas. The Russians also augmented these seizures with cyberspace attacks against Georgian pipelines coupled with a very conveniently timed attack on a Georgian pipeline in Turkey by local militants.[18]

In addition to pipeline attacks, there were further strategic information warfare attacks against the Georgian banking system, which took the entire system down for ten days.[19] According to Robert Pape's typology of coercion, I consider the banking attacks as part of a punishment strategy that the Russians intended to put pressure on both the Georgian people and the Georgian elites.[20] The cyberspace elements of this strategy are

[16] For a complete definition and discussion of what constitutes strategic information warfare, see appendix C.
[17] United States Cyber Consequences Unit, "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008," 7.
[18] United States Cyber Consequences Unit, "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008," 7.
[19] Shakarian, et al., *Introduction to Cyber-Warfare*, Kindle Location 1017, chap 3.
[20] Pape, *Bombing to Win*, 7.

strategic information warfare as they produced effects on physical systems directly from cyberspace. The next step is to quantify these objectives as inputs into the cyberspace superiority measurement model.

I utilized the methodology in appendix A to code the Russian offensive objectives and weighting. Based on the discussion earlier, I identified four Russian objectives, the first of which was to cut Georgian internal communications. The attacks were extremely successful in achieving this objective as it, "was almost impossible for citizens and officials alike to communicate about what was happening on the ground during the military invasion."[21] Russia also successfully shut down Georgian cell phone service, further reducing the capability of Georgians to communicate internally about what was happening.[22] Overall, the Russians were extremely but not completely successful in this area, which equates to $S_1 = 0.90$.

The next Russian objective was to sever Georgian communications with the international community, most likely in an attempt to get their overall campaign objectives achieved before the international community could bring much pressure to bear. Accordingly, they attacked both BBC and CNN with some success.[23] However, with the multiplicity of international communications, Russia was only minimally successful at cutting off information to the international community, which equates to $S_2 = 0.20$.

---

[21] Dan Goodin, "Georgian cyber attacks launched by Russian crime gangs: With help from Twitter, Facebook and Microsoft," *The Register*, 18 August 2009. http://www.theregister.co.uk/2009/08/18/georgian_cyber_attacks/.
[22] Paulo Shakarian, "The 2008 Russian Cyber Campaign Against Georgia." Military Review, November-December 2011, 65.
[23] United States Cyber Consequences Unit, "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008," 5.

The third Russian objective was to shift customers from Georgian to Russian pipelines, I deduce from the order in which the Russians attacked areas of Georgia coupled with the pressure brought on Georgian pipelines through mysterious insurgent attacks in addition to the cyberspace attacks. There was some damage to Georgian credibility and some oil and gas producers did look for alternate routes, but there was not long term impact and the Russians were minimally successful against this objective with $S_3 = 0.20$.[24]

I can infer the final Russian objective from the banking target set. Georgian banks were flooded with fraudulent transactions, which caused international banks to cut Georgia off from the international banking system.[25] This action had the effect of shutting down Georgia's banking system for 10 days, which produced hardship for regular Georgians, but special concern for the Georgian elites who were most affected by banking disruption, and also had the most voice with the government.[26] However, while technically successful, this attack was only minimally successful in accomplishing the Russian objective, as there was no discernable pressure by either elites or regular Georgians on the Georgian government. Accordingly, $S_4 = 0.20$.

I tilted the weighting of the Russian offensive objectives towards cutting internal Georgian communications. I did this because Russian operational success on the ground was of primary importance and if the Georgians had thrown back the Russians, none of

[24] United States Cyber Consequences Unit, "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008," 7.
[25] Shakarian, et al., *Introduction to Cyber-Warfare*, Kindle Location 1014, chap. 3.
[26] Shakarian, et al., *Introduction to Cyber-Warfare*, Kindle Location 1017, chap. 3.

the other objectives would have been very important. Accordingly, I gave cutting internal Georgian communication half of the weighting with $W_1 = 0.50$.

Cutting external Georgian communications and putting pressure on the Georgian government were less important objectives that received less emphasis in the attacks. I weighted these two objectives as twice the weight of the final objective of shifting customers to Russian pipelines. The final pipeline objective only received a limited amount of effort from the Russian cyber attackers and was peripheral to the key issues in the Russian and Georgian conflict. Therefore I set W_2 and $W_4 = 0.20$ each, and $W_3 = 0.10$. Table 3 shows the Russian offensive inputs.

Table 3 – Russian Offensive Objectives in Russian/Georgian Conflict

	Objective	**Level of Success (S)**	**Weighting Factor (W)**
1	Cut Internal Georgian Communications	0.90	0.50
2	Cut External Georgian Communications	0.20	0.20
3	Shift Customers to Russian Pipelines	0.20	0.10
4	Punishment/Pressure Georgia	0.20	0.20

When input into the measurement system, these objectives and weights yield $OCSI_{Russia} = 0.55$, which represents a successful offensive campaign by Russian forces and is the third highest OCSI of the eight cases I examined.

The Georgians were not completely idle on the offensive front, although they did not have nearly the success of the Russians. The Georgians launched two documented attacks of their own, one against South Ossetia in the week before the conflict. In addition, they attempted one known "counter-cyberspace" attack trying to make the

Russian attack blowback on Russia by posting a counterfeit attack tool. This tool acted as if it was attacking Georgian sites while actually attacking Russian ones.[27]

Both Georgian attacks had minimal impact against their targets and had almost no success against their objectives. Thus, in accordance with the coding methodology in appendix A, both S_1 and $S_2 = 0.05$.

It was unclear how much importance the Georgians put into their two objectives of degrading South Ossetian communications and diverting Russian attacks. In the absence of good data, I gave each objective equal weighting so W_1 and $W_2 = 0.50$. In this particular case, the weighting has no real effect on the OSCI since both S_1 and S_2 have the same value. Table 4 gives the Georgian levels of success and weighting.

Table 4 – Georgian Offensive Objectives in Russian/Georgian Conflict

	Objective	**Level of Success (S)**	**Weighting Factor (W)**
1	Degrade South Ossetian Communications	0.10	0.50
2	Divert Russian Cyber Attacks to Russian Targets	0.10	0.50

This weighting yields an $OCSI_{Georgia} = 0.10$ and illustrates that Georgia had little offensive success in this conflict. The offensive side of cyberspace superiority is only half of the story; next, we turn to the defensive aspect.

Defensive Level of Functionality (L) and Criticality (C) in Russia vs. Georgia 2008

On the defensive side of the conflict, the Russians appeared to have little difficulty dealing with Georgian attacks. Only two of their systems came under any

[27] Shakarian, et al., *Introduction to Cyber-Warfare*, Kindle Location 991, chap 3.

Georgian attack at all: their conventional military command and control and their command and control of their cyberspace forces. There is no indication at all that the Georgians had any effect on Russian military command and control so $L_1 = 1.0$. As for the Russian command and control of their cyberspace forces, there was a counterfeit Georgian attack tool operative on some Russian bulletin boards used to control the Russian forces. While there is no evidence that this counterfeit tool had any effect on Russian control of their cyberwarriors, it is likely that the Georgians fooled at least a few. I therefore set $L_2 = 0.90$ which represents negligible degradation in the Russian cyberspace command and control system.

Command and control of their conventional forces was overwhelmingly more important to the Russians than control of their cyberspace assets and I weighted it much heavier when calculating cyberspace superiority. Therefore I set $C_1 = 0.95$ and $C_2 = 0.05$. The Russian side's defensive inputs are in table 5.

Table 5 – Critical Russian Systems in Russian/Georgian Conflict

	System	Level of Functionality (L)	System Criticality (C)
1	Conventional Military Command and Control	1.00	0.95
2	Cyberspace Command and Control	0.90	0.05

These inputs yield a $DCSI_{Russia} = 0.995$ and with rounding to two decimal places, $DCSI_{Russia} = 1.00$, which represents total success for the Russians on the defensive side. The Georgians were far less successful in their defensive efforts.

The Georgians were very ineffective in defending their systems, which contributed to their lack of cyberspace superiority. Georgian cyberspace defenses fell into two broad categories, normal firewall type defenses, and system resilience. The Georgians had normal firewalls and intrusion detection systems in place. These systems were not adequate to stop even the initial wave of Russian attacks. The Georgians sought technical assistance from Estonia and other NATO countries to enhance their defenses but it soon became apparent that they were unable to defend successfully their systems. Georgia then shifted to a reconstitution and resilience mode where they moved their key websites to servers in Estonia and the United States. While this attempt was marginally more successful, they still had great difficulty in keeping their websites accessible.[28] The Russian attackers overcame this attempted block through persistent and simultaneous attacks from multiple botnets, or groups of remotely controlled computers. At one point, the website of the Georgian president was under attack from 500 different IP addresses simultaneously.[29] I have captured the success of these Russian attacks in the Georgian defensive inputs into the measurement system.

The attackers severely curtailed Georgian internal communications with all Georgian cell phone service as well as much of the e-mail system collapsing. As a result I coded the system as barely functional, which equates to $L_1 = 0.10$.

While international communications came under pressure, Georgia was still able to get out some elements of its message. It is clear that international communications were neither mostly functional nor mostly inoperative, but I was unable to find any data

[28] United States Cyber Consequences Unit, "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008," 7.
[29] Rosenzweig, *Cyber Warfare*, Kindle Location 736, chap 3.

detailed enough to develop specific percentages. In the absence of comprehensive data, I assigned $L_2 = 0.50$.

The banking system collapsed completely during the conflict. This makes coding simple, and $L_3 = 0.00$.

The Georgian government lost most of its ability to communicate with its various components through both cyberspace and telecommunications. In accordance with the coding matrix in appendix A, the communications system was minimally functional since some orders still got through and so $L_4 = 0.20$.

Finally, the Georgian infrastructure that came under attack experienced disruption but I was unable to find detailed information about how much. In the absence of detailed data, I estimated a 50% degradation and set $L_5 = 0.50$.

In weighting the system criticality of the Georgian cyberspace systems that came under attack, internal communication was the most important. The lack of internal communication greatly hampered Georgian conventional forces as they attempted to meet the Russian attack. Had the Georgian military been able to mount any sort of effective defense, it would have purchased time and maneuver space for the Georgian government to involve the international community and weakened the bargaining position of the Russians. Accordingly, I set the criticality of the internal communications system at $C_1 = 0.50$ to give it the same weight as the other four systems combined.

The next most important system was international communications. Had the Georgians been able to communicate clearly to the outside world, they could potentially have been able to rally support and international pressure to their assistance. Increased international support would have provided more benefit to the Georgians than improved

access to their other cyberspace systems so I gave international communications twice the weight of the remaining systems with $C_2 = 0.20$.

The remaining three systems of banking, government communication, and infrastructure I gave equal weighting at $C_3 = C_4 = C_5 = 0.10$. While each of these systems was important, none of them had the impact of international or internal communications on the outcome of the conflict. The Georgian systems that came under attack are in table 6.

Table 6 – Critical Georgian Systems in Russian/Georgian Conflict

	System	Level of Functionality (L)	System Criticality (C)
1	Georgian Internal Communications	0.10	0.50
2	International Communications	0.50	0.20
3	Banking	0.00	0.10
4	Government Communication	0.20	0.10
5	Georgian Infrastructure	0.50	0.10

With these inputs, the measurement system produces a $DCSI_{Georgia} = 0.22$. This is on the low end of the eight case studies and represents a relatively unsuccessful defense.

Relative Cyberspace Superiority Index in Russia vs. Georgia

Cyberspace systems were of approximately equal importance to both parties in the Russian/Georgian conflict so I set both Rs to 0.50. There was not a clear distinction between Russia and Georgia in what they use cyberspace for, or how reliant they were upon it.

When I enter all of the previous information into the RCSI equation, it yields:

$OCSI_{Russia} = 0.55$
$DCSI_{Russia} = 1.00$
$R_{Russia} = 0.50$
$OCSI_{Georgia} = 0.10$
$DCSI_{Georgia} = 0.22$
$R_{Georgia} = 0.50$

$CSI_{Russia} = 0.77$ and $CSI_{Georgia} = 0.16$, which yields:

$RCSI_{Russia} = 0.61$
$RCSI_{Georgia} = -0.61$

Russia accomplished a very high level of cyberspace superiority and approached cyberspace supremacy; a condition where Georgia would have had no meaningful capability in cyberspace. Georgia was woefully unprepared for the conflict and apparently expected that Russia would not react as vigorously as it did. In addition, Georgia may have expected the United States or the EU to provide more forceful assistance; however, the Western nations had warned Georgia not to provoke a conflict, and so did not provide significant support.

I combined the various elements used in this attack and they follow in figure 12.

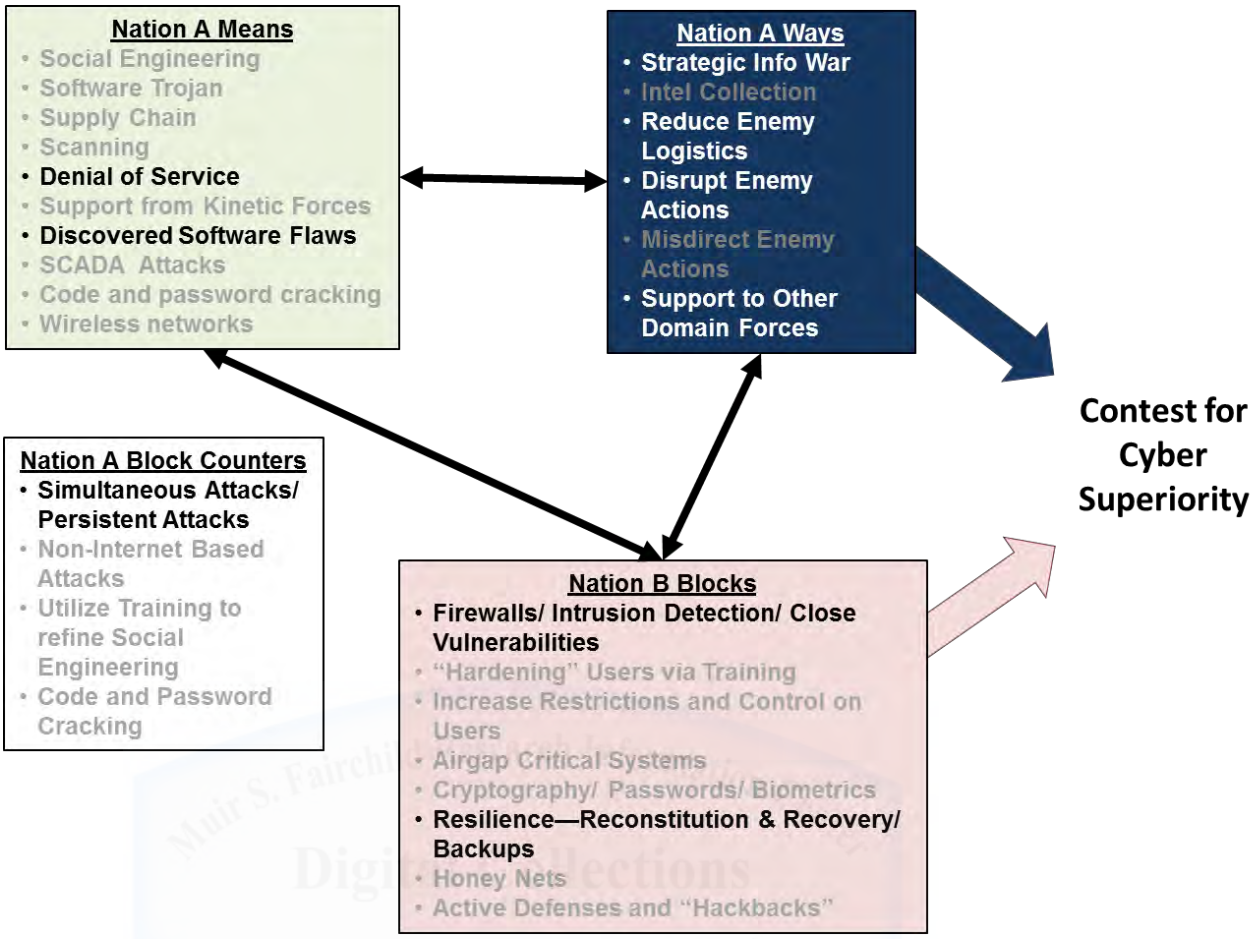

Figure 12 –Russian Cyberspace Superiority in 2008 versus Georgia
Source: Author's Original Work

The Russians were able to overcome Georgian defenses to establish a significant level of cyberspace superiority. The Russians principally relied upon denial of service and discovered software flaws to get through the first layer of Georgian defenses and persistent and simultaneous attacks to deal with Georgian attempts at resilience. This cyberspace superiority brought benefits to Russian forces.

Russian forces were able to capitalize on their opponent's lack of ability to communicate. While Russian airborne forces performed creditably, their regular forces

did not all perform well.[30] Had Georgian forces been able to communicate, it is conceivable that they could have been far more effective at the operational level. Had the Georgians been able to block the Roki tunnel for example, it would have had a significant impact on the speed with which Russia could flow troops into the contested area.[31] The advantage enjoyed by Russian forces because of their cyberspace superiority is of great importance to this study.

Given that the Russian-Georgian conflict is the only case currently available to study that incorporated both cyberspace attacks and conventional military operations, the linkage between cyberspace superiority and Russian conventional success is significant. Given the great disparity in forces and strategic preparation, Russia would likely have been successful even without the achievement of cyberspace superiority. However, Russian military forces clearly enjoyed benefits from their cyberspace superiority, particularly in the inability of the Georgians to communicate and coordinate their actions. The Russians also derived some benefits from their cyberspace superiority at the strategic level.

On the strategic level, Russian cyberspace superiority made it easier for the Russians to accomplish their objectives before the international community really understood what was happening. Presenting the international community with a *fait accompli* made it much harder for other states to intervene to change the situation and allowed Russia to achieve many of its strategic goals in Georgia. The next case study of

[30] Ariel Cohen and Robert E. Hamilton, *The Russian Military and the Georgia War: Lessons and Implications* (Carlisle, PA: Strategic Studies Institute, 2011), 27.
[31] Cohen and Hamilton, *The Russian Military and the Georgia War*, 19.

Stuxnet had very different characteristics than the Georgian attacks and sought a different type of operational advantage.

Stuxnet

Stuxnet is an important case to examine for this study, as it was the first known example of a cyberspace weapon that produced physical effects. On 17 June 2010, researchers at a small Belarusian computer security firm discovered a new piece of malicious software or malware infecting USB memory sticks.[32] That malware, which analysts eventually named Stuxnet based on a name found in the code, was the world's first precision cyberspace weapon designed to have effects outside of cyberspace in the other physical domains.

Stuxnet was not a normal piece of malware that hackers in a basement or even a criminal syndicate put together. Prior to Stuxnet, no piece of malware had utilized more than one, zero-day vulnerability.[33] The complicated "Aurora" malware, responsible for attacks on Google in late 2009, and every other known piece of malware prior to Stuxnet, had relied on, at most, one zero-day vulnerability.[34] Most attacks do not have a single zero-day vulnerability and are instead built around known vulnerabilities. Stuxnet utilized five separate zero-day vulnerabilities and was far more complex than anything that security experts had discovered before.[35] It also did not appear as if the designers of

[32] Aleksandr Matrosov, Eugene Rodionov, David Harley, and Juraj Malcho, "Stuxnet Under the Microscope: Revisions 1.31," *eSeT*. Accessed 25 August 2013. http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf. 19.
[33] For a discussion of "zero-day" vulnerabilities, see appendix C in the section on discovered software flaws.
[34] Paulo Shakarian, "Stuxnet: Cyberwar Revolution in Military Affairs," *Small Wars Journal*, 15 April 2011. 6.
[35] Matrosov et al., "Stuxnet Under the Microscope: Revisions 1.31," 7.

Stuxnet intended it for the traditional criminal activities such as spam or fraud. According to Paulo Shakarian, "other malware include standard code for a variety of criminal activities – including identity and password theft, launching denial-of-service attacks, and sending spam emails. Despite its high degree of technical sophistication, Stuxnet was not designed to perform any of these activities."[36]

What Stuxnet was designed to do was to alter the instructions that were sent to a Siemens S7-417 or S7-315 industrial controller, but only if the controller was attached to a very specific configuration of devices.[37] Given that security researchers discovered the majority of infections in Iran, and the fact that Iran had configured their nuclear centrifuges in exactly the manner specified in Stuxnet, a motive and likely suspects were easy to come by.

Offensive Level of Success (S) and Weighting Factor (W) in the Stuxnet Case

The first input into the cyberspace superiority measurement model is the objectives of the attacker, thus the identity of the attacker is the first aspect of this case we need to determine. Analysts immediately suspected that the United States and Israel were behind Stuxnet in an attempt to slow the development of an Iranian nuclear weapon. Experts determined that two organizations wrote Stuxnet based on their analysis of the code. The New York Times published a story reporting this claim and its connections to the administration.[38] The United States and Israel have not directly admitted to creating and deploying Stuxnet, but for the purposes of this study, the attribution is likely enough

[36] Shakarian, "Stuxnet: Cyberwar Revolution in Military Affairs," 2.
[37] Shakarian, "Stuxnet: Cyberwar Revolution in Military Affairs," 2.
[38] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, 1 June 2012.

to proceed. David Sanger, the New York Times reporter, has written a book, which provides extensive detail on the decisions behind the development and deployment of Stuxnet. The government has not confirmed Sanger's story, but they are trying to figure out who gave him the information so that the Justice Department can prosecute the leaker.[39] Accordingly, attributing the attack to the United States and Israel in accordance with Sanger's reporting seems reasonable. Now that the identity of the attackers has been determined, we turn next to what their objectives were.

Based on American and Israeli policy and messaging, it appears that the overall objective of Stuxnet was to slow the Iranian nuclear program to provide time for sanctions and negotiation to solve the problem. Thus, the first objective was to delay enrichment activities at Natanz as much as possible by sabotaging the enrichment system. It also appears the attackers wanted effects beyond temporary disruption.

The attackers did not just want to stop current enrichment activities; they wanted physically to destroy equipment to prevent future enrichment. As evidence of this, it appears that Stuxnet escaped "into the wild" because the attackers began to utilize a more aggressive attack method when they were not achieving a high enough level of destruction.[40] It appears that the more aggressive version of Stuxnet got out in the wild when an Iranian scientist inadvertently interrupted Stuxnet in the middle of a process. This interruption resulted in Stuxnet spreading beyond the nuclear system the designers

[39] Rowan Scarborough, "In classified cyberwar against Iran, trail of Stuxnet leak leads to White House," *The Washington Times*, 18 August 2013.
[40] Shakarian, et al., *Introduction to Cyber-Warfare*, Kindle Location 6972, chap. 13.

intended it exclusively to infect.[41] This mistake resulted in the attacker's failure to accomplish their third objective of secrecy.

A third objective was clearly to remain undetected as long as possible. One of the most impressive aspects of Stuxnet was that it not only destroyed centrifuges, it made it look like the centrifuges were dying of "natural causes." Stuxnet periodically changed the speed of the centrifuges in a specific manner designed to produce eventual failure, but continued to report to the controller that everything was fine and the centrifuge was spinning exactly as it should.[42] Part of the objective of Stuxnet was not just to delay, but also to confuse and mystify the Iranians as to why their centrifuges were not working, which would produce even more delay.[43] This was only possible as long as the weapon itself remained hidden.

The attackers only had mixed success against these objectives. On the one hand, it appears that there was damage done to Iranian centrifuges. Iran decommissioned and replaced about 1,000 IR-1 centrifuges at the Natanz Fuel Enrichment Plan in late 2009 or early 2010.[44] Stuxnet could easily have been responsible for the destruction of these centrifuges. It is also verifiable that while the Iranians designed Natanz for 50,000 centrifuges, there were only about one fifth of that number running after ten years of work.[45] On the other hand, the Iranians apparently responded to the reduction in efficiency by significantly ramping up the number of centrifuges they were running. The Iranians managed to increase their daily production by 20%, although the Institute for

[41] Sanger, *Confront and Conceal*, 204.
[42] Shakarian, "Stuxnet: Cyberwar Revolution in Military Affairs," 3.
[43] Sanger, *Confront and Conceal*, 199.
[44] Shakarian, et al., *Introduction to Cyber-Warfare*, Kindle Location 6943, chap. 13.
[45] Sanger, *Confront and Conceal*, 207.

Science and International Security (ISIS) report considered this a significant underperformance given the number of new centrifuges the Iranians added.[46]

The delay in the enrichment program was significant, but it also was not everything the Stuxnet attackers were hoping to accomplish. The estimates of how long Stuxnet delayed the Iranian nuclear program vary from about one to three years, which still represents significant success.[47] Therefore, I coded $S_1 = 0.50$ in accordance with the coding methodology in appendix A.

Based on the number of centrifuges taken offline and replaced at Natanz while the attack was operable, it is clear that Stuxnet was at least partially successful in destroying equipment. However, it appears that the destruction was not sufficient to stop completely the Iranian program as the Iranians introduced more than enough centrifuges to compensate and actually increased their production. The Iranian increase in production does not automatically imply that the attackers were unsuccessful. Stuxnet evidently affected uranium production significantly, as the Iranians should have been able to produce far more enriched uranium than they did with the number of centrifuges they were operating. Thus, Stuxnet's success against destroying equipment is mixed with $S_2 = 0.50$.

The final objective for Stuxnet was to remain hidden. Unfortunately for the attackers, Stuxnet was not only found by the defenders, but also got out into the wild where numerous researchers took it apart and analyzed it. Therefore I set $S_3 = 0.0$ as a complete failure of the objective. This coding might seem unduly harsh as Stuxnet did

[46] Shakarian, et al., *Introduction to Cyber-Warfare*, Kindle Location 6945, chap. 13.
[47] Sanger, *Confront and Conceal*, 207.

remain undetected for two to three years, but the decision to "swing for the fences" resulted in the attack having a shorter life span than desired.[48] Once researchers had discovered Stuxnet, the Iranians were able to get their program back on track.

Since delaying the Iranian nuclear program was the main strategic purpose behind Stuxnet, I gave it as much weight as the other two objectives combined. Therefore, I set $W_1 = 0.50$.

Of the two remaining objectives, doing damage was apparently more of a priority than staying hidden. I can deduce this from the fact that Stuxnet was "torqued-up" in order to do more damage despite the fact that the upgrade would increase the risk of exposure.[49] Accordingly I set $W_2 = 0.3$ and $W_3 = 0.2$. The inputs on the offensive side of the Stuxnet attack are in table 7.

Table 7 – US/Israeli Objectives with Stuxnet versus Iran

	Objective	**Level of Success (S)**	**Weighting Factor (W)**
1	Delay Current Iranian Nuclear Enrichment	0.50	0.50
2	Destroy Iranian Nuclear Enrichment Equipment	0.50	0.30
3	Remain Undetected	0.00	0.20

Given these inputs, $OCSI_{US/Israel} = 0.40$. This value is in the lower range of OCSIs in the case studies among those nations who were actively attacking. Since the Iranians were not actively attacking as part of this conflict during this timeframe, I set $OCSI_{Iran} = 0.00$.

[48] Sanger, *Confront and Conceal*, 204.
[49] Sanger, *Confront and Conceal*, 204.

Defensive Level of Functionality (L) and Criticality (C) in the Stuxnet Case

The next step in analyzing the Stuxnet attacks is to determine the defensive inputs for the cyberspace superiority measurement model. The Iranians expected that their facilities would come under attack and so worked hard to protect their systems as much as possible. It is reasonable to assume that the Iranians had protected the Internet-enabled computers in the facilities with firewalls and intrusion systems. Given the high security present in the facility, coupled with the suspicions of sabotage, it is also likely that there were significant restrictions and controls on users. One of the methods relied upon by the Iranians to block attackers was reconstitution and recovery. Despite losing at least a thousand centrifuges and a major reduction in efficiency of production, they brought in many more centrifuges and actually managed to increase production.[50] Additionally, in Supervisory Control and Data Acquisition (SCADA) systems such as the one attacked by Stuxnet, air gapping is normally a key defense.

It also appears that the controllers running the centrifuges were air gapped and not directly connected to the Internet.[51] The structure and design of Stuxnet confirms the Iranian air gap, as the attackers clearly designed Stuxnet to jump an air gap utilizing multiple methods. Stuxnet has four different propagation methods that include flash drives and various wireless and wired network attacks.[52] The designers of Stuxnet also used persistence to continue to hammer away at the air gap. Security researchers have found several different versions of Stuxnet dating back as far as 2007 and it appears that

[50] Shakarian, et al., *Introduction to Cyber-Warfare*, Kindle Location 6945, chap. 13.
[51] Sanger, *Confront and Conceal*, 194.
[52] Matrosov et al., "Stuxnet Under the Microscope: Revisions 1.31," 24.

the designers continued to make changes to increase the effectiveness of the attack.[53] While the designers of Stuxnet were after the SCADA system, they understood that the road to it lay through the support system.

The two systems Iran was trying to defend in Natanz were the support system network of computers and the SCADA control systems themselves. The support system network consisted of the computers in the facility used to support the enrichment process and was the system Stuxnet needed to infiltrate to get to the SCADA system. The SCADA controllers ran the actual process, which was the point of the facility.

It appears that the attackers had riddled the support computer system with Stuxnet, which was also extremely hard to get rid of, as a single infected device missed by the defenders would rapidly infect the entire network all over again. The purpose of the support system was to keep the SCADA system operational and functioning. Instead of providing defense and support, the support system was the avenue through which the SCADA system was attacked, thus I set $L_1 = 0.00$.

It is harder to assess the level of functionality of the Natanz SCADA system, as there is no reliable, unclassified data available. It does appear that the Iranians had a very difficult time getting Stuxnet out of their systems and they temporarily shut down enrichment operations at Natanz in November 2010.[54] I have to balance this data with the fact that overall enrichment numbers continued to rise over time due to a massive influx of new centrifuges so the system maintained at least some capability. However, given that the SCADA system was under the control of an enemy and was actively

[53] Jim Finkle, "Researchers say Stuxnet was deployed against Iran in 2007," *Reuters*, 26 February 2013. http://www.reuters.com/article/2013/02/26/us-cyberwar-stuxnet-idUSBRE91P0PP20130226.
[54] Shakarian, et al., *Introduction to Cyber-Warfare*, Kindle Location 7003, chap. 13.

working to destroy centrifuges while allowing just enough enrichment to remain undetected, I set the level of functionality of the system as barely functional with $L_2 = 0.10$.

Of the two systems, the SCADA system was the heart of the uranium enrichment process and the support system was less important in the day-to-day process. I put four times the weight on the SCADA system versus the support system and so set $C_1 = 0.20$ and $C_2 = 0.80$. The inputs on the defensive side are in table 8.

Table 8 – Iranian Systems in Stuxnet Attack

	System	Level of Functionality (L)	System Criticality (C)
1	Support System Network	0.00	0.20
2	SCADA Control System	0.10	0.80

Given these inputs, $DCSI_{Iran} = 0.08$. This is a very low level of defensive cyberspace superiority when compared to the other case studies. Since the Iranians were not directly counter attacking the US and Israel had a $DCSI_{US/Israel} = 0.00$.

Relative Cyberspace Superiority Index in the Stuxnet Case

I set $R_{US/Israel} = 0.75$ and $R_{Iran} = 0.25$ based on the greater level of importance of cyberspace in U.S. and Israeli society. The complete list of variables is as follows:

$OCSI_{US/Israel} = 0.40$
$DCSI_{US/Israel} = 0.00$
$R_{US/Israel} = 0.75$
$OCSI_{Iran} = 0.00$
$DCSI_{Iran} = 0.08$
$R_{Iran} = 0.25$

$CSI_{US/Israel} = 0.10$ and $CSI_{Iran} = 0.02$, which yields:

$RCSI_{US/Israel} = 0.08$
$RCSI_{Iran} = -0.08$

It is interesting to note that giving Stuxnet full credit for remaining undetected and setting $S_3 = 1.0$ only changes the overall $RCSI_{US/Israel}$ slightly to 0.13. Either way, this RCSI represents a very low level of cyberspace superiority by the U.S. and Israel, which makes sense given that despite whatever damage the attackers did, Iran's production of enriched uranium appears to have actually increased slightly.

These numbers represent a "best case" scenario for the U.S. and Israel. Since the level of success is not clear, I also ran a case with:

Iranian $L_1 = 0.50$
Iranian $L_2 = 0.50$

This scenario represents a more successful defense by Iran with them maintaining 50% effectiveness in both their support and SCADA systems. It is not likely that the Iranians achieved more than 50% system functionality given the evidence of disruption discussed previously. In this case, the variables become:

$OCSI_{US/Israel} = 0.40$
$DCSI_{US/Israel} = 0.00$
$R_{US/Israel} = 0.75$
$OCSI_{Iran} = 0.00$
$DCSI_{Iran} = 0.50$
$R_{Iran} = 0.25$

$CSI_{US/Israel} = 0.10$ and $CSI_{Iran} = 0.13$, which yields:

$RCSI_{US/Israel} = -0.03$
$RCSI_{Iran} = 0.03$

In this case, Iran has a very slight cyberspace superiority. It appears that Stuxnet most likely represented a low level of cyberspace superiority for the U.S. and Israel, as

they achieved some of their objectives, but it is possible that it represented something closer to parity with neither side having superiority.

Stuxnet was a complex attack that utilized multiple attack vectors. A depiction of the Stuxnet attack is in figure 13.

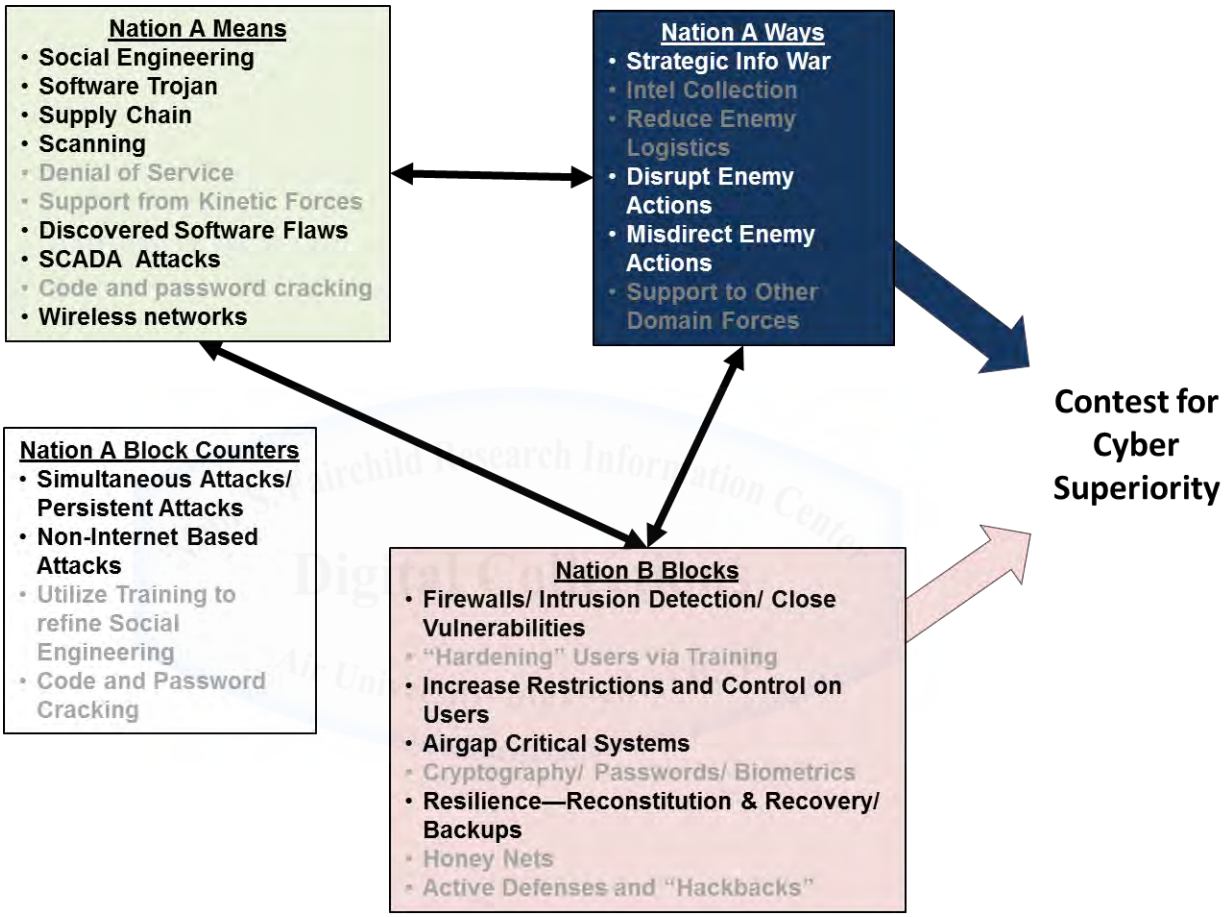

Figure 13 – Stuxnet attack on Iranian Nuclear Systems
Source: Author's Original Work

Because Stuxnet is such a flexible piece of malware that has multiple propagation pathways, it is difficult to say with certainty which pathway was the effective one. The attackers may have initially inserted Stuxnet into Iran via social engineering, or supply chain attacks. Either way, the designers clearly intended for it to spread across wireless

networks. Once in place, it became a software Trojan and utilized multiple software flaws to execute SCADA attacks on industrial controllers. The attackers overcame Iranian attempts to block Stuxnet from interfering with their SCADA systems by using non-Internet based methods to jump the air gap combined with persistence by the attackers. Several of these characteristics are unique to Stuxnet so far, and important to cyberspace superiority.

Stuxnet was the first cyberspace weapon that demonstrated the capability to leverage cyberspace superiority to produce effects in the physical world. Researchers had generated physical effects in laboratory settings, but Stuxnet is the first case where attackers utilized such a weapon. Stuxnet will likely not be the last cyberspace attack to generate effects in the physical world and the fact that analysts discovered the weapon and propagated the source code makes it even more likely that lower level nation-state attackers can study Stuxnet and develop similar weapons to suit their objectives.

Stuxnet was the first major cyberspace attack by a nation state to use cyberspace superiority to target SCADA systems. SCADA attacks on power grids and infrastructure have been a constant theme of authors trying to raise public interest, and public funding, for cyberspace; but prior to Stuxnet, these types of attacks were mostly theoretical. Stuxnet demonstrated that attacks on SCADA systems are a real threat, even to the most highly guarded and defended systems.

Stuxnet was the first cyberspace weapon known to have successfully breached an air gap defense. Prior to Stuxnet, analysts had considered air gaps an effective defense against attackers and a good way for defenders to maintain cyberspace superiority over their critical systems. Stuxnet demonstrated that there are ways around air gaps, and even

provided the details for potential future attackers since researchers released the source code.

Stuxnet is the only known case of a nation-state maintaining some level of cyberspace superiority over an extended period. The designers of Stuxnet accomplished this by keeping Stuxnet hidden and masking its effects by making the failures look random and a result of poor design and workmanship. There is a natural tension in this approach between how effective the weapon is, and how long it can stay hidden. The more effective the weapon, the more likely a defender will discover it. In the Stuxnet case, defenders discovered it as a direct result of Stuxnet's designers releasing a more aggressive variant. The attackers' strategy of obscuration may not be available in all cases, but when it is available, it can produce long duration cyberspace superiority. The final case study is one where Stuxnet's Iranian defenders attempted to utilize some aspects of what they learned to attack Saudi Arabia, albeit with less success.

Aramco

On 15 August 2012, attackers using a computer virus named Shamoon infected the Saudi Arabian national petroleum company Aramco.[55] This attack was not typical corporate espionage; the attackers intended to be as destructive as possible and ended up disabling 30,000 computers.[56] Shamoon did not have provisions for stealing information and it did not appear that the attackers were targeting specific individuals. The characteristics of the attack provide important hints as to who was likely behind it.

[55] Christopher Bronk and Eneken Tikk-Ringas, "Hack or Attack? Shamoon and the Evolution of Cyber Conflict," James A Baker III Institute for Public Policy Working Paper, 1 February 2013.
[56] Shakarian, et al., *Introduction to Cyber-Warfare*, Kindle Location 1875, chap. 5.

Offensive Level of Success (S) and Weighting Factor (W) in the Aramco Case

As before, the first question is who was behind the attack as their objectives are a key input into the cyberspace superiority measurement model. The weight of the evidence suggests that Iran was behind the attack. The evidence is not conclusive, at least at the unclassified level, but the perennially nameless "American intelligence officials," have blamed Iran for the attack.[57] In addition, Secretary of Defense Leon Panetta made a number of veiled remarks interpreted as holding Iran responsible without directly accusing Iran.[58] Jeffrey Carr has done the most detailed analysis on attribution for Aramco that is available in the open press and he too concludes that Iran was most likely behind the Shamoon virus.[59] Both the "Arab Youth Group" and the "Cutting Sword of Justice" are groups that claimed responsibility for the attack, accusing Saudi Arabia of oppression. Either group, or both, could be fronts for the Iranian Cyber Army (ICA), allegedly, "created in 2005 as part of the Iranian Revolutionary Guard Corps

[57] Thom Shanker and David E. Sanger, "U.S. Suspects Iran Was Behind a Wave of Cyberattacks," *New York Times*, 13 October 2012. http://www.nytimes.com/2012/10/14/world/middleeast/us-suspects-iranians-were-behind-a-wave-of-cyberattacks.html?_r=2&pagewanted=all.

[58] Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *The New York Times*, 23 October 2012. http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all.

[59] To quote his analysis fully, "Iran is at the center of every significant aspect of this attack. It is the only nation with access to the original Wiper virus from which Shamoon was copied. Iran is angry at Saudi Aramco for off-setting Iran's drop in oil production due to the Embargo that started 45 days prior to the attack which gives it motive. It supports a militant organization (Hezbollah) that uses hackers and who allegedly has members employed at Saudi Aramco which gives it opportunity and access. While both the Arab Youth Group and the Cutting Sword of Justice involvement gives it the appearance of a mere hacktivist attack, I think that a careful analysis of the known facts points to a state-sponsored attack by Iran that was crafted to look like the work of hacktivists. Perhaps Iran has learned something from Russia about the strategy of misdirection via the government's recruitment of patriotic hackers." Jeffrey Carr, "Who's Responsible for the Saudi Aramco Network Attack?" *Infosec Island*, 28 August 2012. http://www.infosecisland.com/blogview/22290-Whos-Responsible-for-the-Saudi-Aramco-Network-Attack.html.

(IRGC)."[60] While this evidence is strong, there is one factor some analysts point to as a counter to this line of reasoning.

The evidence that some experts use to argue that Iran was not behind the attack is the inclusion of a reference to the "Arabian Gulf" in the code.[61] Given the Iranian obsession with ensuring that everyone in the world calls that particular body of water the "Persian Gulf," some have claimed that this evidence shows Iran was not behind the attack. I do not find this piece of evidence persuasive, as it would have been very easy for the programmers to include that reference for the specific reason of throwing off analysts given the high level of Iranian cultural significance in the phrase. Americans may not be familiar with the dispute over the name, but every Iranian is. Accordingly, I attribute the attack to Iran. The defender in this case was a company, but one that the Saudi Arabian government owns and is closely associated with; therefore, I consider this case to be an attack by the government of Iran on the government of Saudi Arabia. The Iranians also intended Shamoon to be far more destructive than mere vandalism.

One important clue to the Iranian objectives in the Aramco case is the high level of destruction intended by the weapon. Shamoon attempted to disable computers by erasing their master boot records.[62] If an attacker succeeds in deleting this information, the computer system cannot start. The computer is disabled and the data on the hard drive is un-accessible without significant effort by specialists. This attack could have been much more serious than one that simply requires reloading software on computers. Had the attacker been successful in getting to the computers running industrial processes,

[60] Shakarian, et al., *Introduction to Cyber-Warfare*, Kindle Location 1856, chap. 5.
[61] Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back."
[62] Shakarian, et al., *Introduction to Cyber-Warfare*, Kindle Location 1856, chap. 5.

any process from pumping to refining could have gone haywire with catastrophic consequences. The type of attack gives insight into the most likely objective of the Aramco attack.

Given the scope of the attack, the state of relations in the Persian Gulf, and the mechanisms built into Shamoon, the most likely goal of the attackers was to disrupt Saudi-Arabian oil and gas production. The groups that did claim the attack, which were likely Iranian front groups, were not very clear on why they were attacking or what they intended to accomplish. According to Abdullah al-Saadan, Aramco's vice-president for corporate planning, "The main target in this attack was to stop the flow of oil and gas to local and international markets."[63]

Another possible motive was to damage the support system computers that the attacker infected with Shamoon. I needed to consider this objective, as the support system is the one that Shamoon ended up affecting. While the attack appeared successful, it was only successful against one of the two objectives.

In some ways, the Aramco attack was a great success as the attacker damaged 30,000 computers; however, the attacker was unable to interfere with production. In its effort, it appears that Iranians attempted to get past the air gap to the production computers. However, this attempt failed and no production computers were infected. Coding the inputs in this case is straightforward. Because the production system remained untouched, petroleum production was unaffected by the attack, the $S_1 = 0.00$, as a complete failure. At the opposite end of the spectrum, Shamoon disrupted 30,000

[63] Abdullah al-Saadan speaking to local media quoted in Camilla Hall and Javier Blas, "Aramco cyber attack targeted production," *Financial Times*, 10 December 2012. http://www.ft.com/intl/cms/s/0/5f313ab6-42da-11e2-a4e4-00144feabdc0.html#axzz2dfwhMlKi.

support system computers and brought the entire support system to a complete halt. Aramco appears to have been mostly off-line for about two weeks from 15 to 28 August 2012.[64] Therefore, I assigned $S_2 = 1.00$, as a complete success. With such wide disparity in success between the two objectives, weighting becomes even more important.

Success against the petroleum production system would have brought Iran far greater strategic benefits than that which they accrued via the support system attack; therefore, I weighted the petroleum production objective much more highly. I assigned four times the weight to disrupting petroleum production as I did to disrupting the support system. Thus $W_1 = 0.80$ and $W_2 = 0.20$. The offensive inputs in the Aramco attack are in table 9.

Table 9 – Iranian Objectives in Aramco Attack

	Objective	**Level of Success (S)**	**Weighting Factor (W)**
1	Interrupt Aramco Petroleum Production	0.00	0.80
2	Damage Aramco Support Network	1.00	0.20

With these inputs $OCSI_{Iran} = 0.20$, which represents a low level of success and cyberspace superiority. This OCSI is the second lowest of the eight cases I examined. On the Saudi Arabian side, the lack of offensive cyberspace objectives yields an $OCSI_{Saudi\ Arabia} = 0.00$. Aramco's defenders had some effective tools in place to protect their systems and now we turn to the defensive inputs.

[64] Holden, "Cyber Attacks in the Spin Cycle: Saudi Aramco and Shamoon," *Analysis Intelligence*, 1 November 2012. http://analysisintelligence.com/cyber-defense/narrative-of-a-cyber-attack-saudi-aramco-and-shamoon/.

Defensive Level of Functionality (L) and Criticality (C) in the Aramco Case

The next main input into the cyberspace superiority measurement model is the level of functionality and criticality of the defended systems. Aramco had significant defenses in place to protect their systems. According to Al-Saadan, the attack did not succeed because, "we had in place the processes and systems to manage, as well as sufficient incident response and business continuity plans to deal with such an attack."[65] He continued and said, "Built-in system architecture and protections for the primary components of our computer network, including firewalls and segmentation, meant that all our core operations continued smoothly."[66] While their "core operations" ran smoothly, they were offline for approximately two weeks so there was significant impact to their support system as noted earlier. This data gives straightforward coding of the defensive inputs.

As the petroleum production computer system appeared to be untouched by the attack and operating at full efficiency, I coded $L_1 = 1.00$. While Aramco had motive to cover up any damage done to their production systems, there was no drop in production apparent to analysts so it appears that Shamoon truly did not reach the production system. This outcome is in stark contrast to that for the support system.

Aramco's support computer system completely collapsed for about two weeks and so the coding of its functionality is relatively simple as well. I coded the support system at $L_2 = 0.00$. Due to the large disparity in functionality between the two systems under consideration, once again the weighting largely determined the output.

[65] Siraj Wahab, "Cyber Attack on Aramco A 'Global Plot', says Saudi Arabia," *Arab News*, 10 December 2012. http://www.eurasiareview.com/10122012-cyber-attack-on-aramco-a-global-plot-says-saudi-arabia/.
[66] Wahab, "Cyber Attack on Aramco A 'Global Plot', says Saudi Arabia."

From a defensive perspective, the petroleum production computer system was far more important to Aramco than their support system. I therefore gave it a similar weight as on the offensive side and I weighted the petroleum production system at four times the importance of the support system. This gives $C_1 = 0.80$ and $C_2 = 0.20$. While the damage to the support system was embarrassing, it did not cause investors to flee Aramco or delay the delivery of any of their product, which would likely have been the case if the attack had affected production. The Saudi Arabian systems inputs in the Aramco attack are in table 10.

Table 10 – Saudi Arabian Systems in Aramco Attack

	System	Level of Functionality (L)	System Criticality (C)
1	Petroleum Production System	1.00	0.80
2	Support Network System	0.00	0.20

These inputs combined yield a $DCSI_{Saudi\ Arabia} = 0.80$. This represents a very successful defense and is the second highest DCSI of the eight cases I analyzed. Iran did not have to defend their systems from Saudi Arabia during this attack and so $DCSI_{Iran} = 0.00$.

Relative Cyberspace Superiority Index in the Aramco Case

Iran and Saudi Arabia are dependent on cyberspace at roughly the same level so R_{Iran} and $R_{Saudi\ Arabia}$ were each set to 0.50. The inputs and final result was:

$OCSI_{Iran} = 0.20$
$DCSI_{Iran} = 0.00$
$R_{Iran} = 0.50$
$OCSI_{Saudi\ Arabia} = 0.0$
$DCSI_{Saudi\ Arabia} = 0.25$
$R_{Saudi\ Arabia} = 0.50$

CSI_{Iran}= 0.10 and $CSI_{Saudi\ Arabia}$ = 0.40, which yields:

$RCSI_{Iran}$ = -0.30
$RCSI_{Saudi\ Arabia}$ = 0.30

Cyberspace superiority for Saudi Arabia makes intuitive sense given that the attack did not affect petroleum production. Aramco's aggressive defensive posture and a successful air gap helped them avert what could have been a catastrophic attack. The attack and the blocks put into place by Aramco are in figure 15.

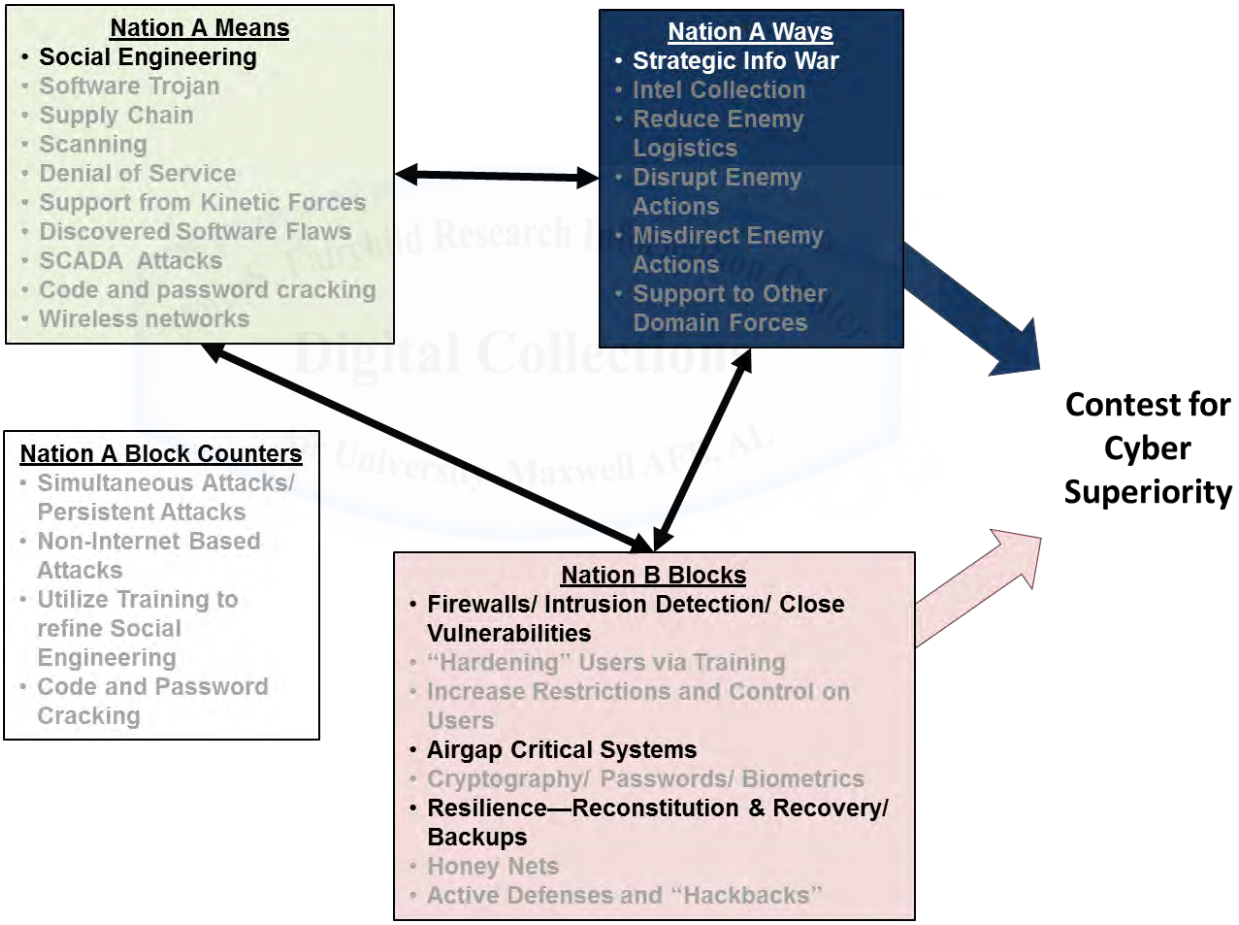

Figure 14 – Iranian Attack on Aramco
Source: Author's Original Work

The principal dynamic apparent from this illustration is that Aramco's air gap prevented the attackers from obtaining their objectives. From some of al-Saadan's public statements, we know that Aramco had firewalls deployed as well as an air gap for their production system, which Al Saadan referred to as "segmentation." It is also clear that there was a reconstitution plan in place for resilience and the New York Times reported that Saudi Arabia flew in a dozen computer experts to help them mitigate the attack and reconstitute systems.[67] The attacker's attempt to use non-Internet propagation to get across the air gap failed, which is why it is still grayed out in figure 15. Another attempted maneuver by the attackers was an additional attack launched on 22 August, one week after the first attack.[68] This second attack fizzled and appears to have done no significant damage, thus the persistence counter in the figure is still gray. One area that is unclear is what delivery mechanism was used by the attackers.

There are two different theories about how the attackers introduced Shamoon into Aramco. The *Wall Street Journal* and *New York Times* reported sources that stated that an insider threat carried it into Aramco on a USB memory stick.[69] The fact that there were 70 Aramco employees Saudi Arabia was investigating for the attack supports this theory.[70] On the other hand, in an interview with *Arab News* al-Saadan denied that there was any insider threat and claimed that it was a "spear-phishing" attack where attackers target an individual with a legitimate looking e-mail that actually downloads malware.[71]

---

[67] Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back."
[68] Holden, "Cyber Attacks in the Spin Cycle."
[69] Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back."
[70] Carr, "Who's Responsible for the Saudi Aramco Network Attack?"
[71] Wahab, "Cyber Attack on Aramco A 'Global Plot', says Saudi Arabia."

Bloomberg also reported this same e-mail story.[72] It is impossible to tell, with the data available, as to which story is correct. It may be that they are both correct in that the virus was initially introduced via a "spear-phishing" attack, but it was designed to spread via USB flash devices in the hopes that it would cross the air gap to the computers that run oil and natural gas production. Like the Russian and Georgian conflict, as well as Stuxnet, there are several important elements of the Aramco attack for cyberspace superiority.

In a several ways, the Aramco attack was very similar to Stuxnet, but with a very different outcome. Shamoon attempted to cross an air gap, but unlike Stuxnet failed to do so. Shamoon was attempting to target a SCADA system, but unlike Stuxnet, it failed to get into the system. Shamoon was different from Stuxnet in that its designers used a less sophisticated approach.

Instead of attempting carefully to manipulate the SCADA system, Shamoon's designers intended it to disrupt the entire SCADA system by irrecoverably crashing individual computers. If Stuxnet was the cyberspace equivalent of a highly trained saboteur sneaking into a facility, Shamoon was an attempt to simply burn down the entire building. Burning down the facility can be effective, but it makes a lot of noise and is impossible to hide.

Shamoon's lack of success in achieving its objectives shows that a well-executed defense that maintains cyberspace superiority can stop a significant cyberspace attack. This lesson is perhaps the most significant finding from the Aramco case study.

[72] Wael Mahdi, "Saudi Arabia Says Aramco Cyberattack Came From Foreign States," *Bloomberg,* 9 December 2012. http://www.bloomberg.com/news/2012-12-09/saudi-arabia-says-aramco-cyberattack-came-from-foreign-states.html.

Disciplined defenders can gain a significant advantage for operations. In this case, they were able to protect significant Saudi Arabian oil and gas infrastructure and economic interests from serious disruption by an enemy state's military. Now that we have examined three case studies in detail, I will present the results of my analysis from all eight case studies.

Analysis of the Case Study Results

A summary of all the cases that met my research criteria is in table 11. Note that analysis to explain the development of the RCSI values for the other cases listed in the table is available in appendix B.

Table 11 – Cyberspace Superiority Case Studies

Year	Case	Presumed Attacker	Objective	Defender	Outcome
2007	Estonia	Russia	Replace Statue, Intimidate Former USSR States	Estonia	$RCSI_{Russia} = (-0.15)$ $RCSI_{Estonia} = 0.15$
2008	Georgia	Russia	Seize South Ossetia and Abkhazia	Georgia	$RCSI_{Russia} = 0.61$ $RCSI_{Georgia} = (-0.61)$
2009	South Korean/ US DDoS	North Korea	Shut down US and South Korean Websites	South Korea/US	$RCSI_{North\ Korea} = (-0.46)$ $RCSI_{US/South\ Korea} = 0.46$
2010	Stuxnet	US/Israel	Disrupt Iranian Uranium Enrichment	Iran	$RCSI_{US/Israel} = 0.08$ $RCSI_{Iran} = (-0.08)$
2011	March 2011 South Korean DDoS	North Korea	Shut down US/South Korean Gov Websites	South Korea	$RCSI_{North\ Korea} = 0.03$ $RCSI_{South\ Korea} = (-0.03)$
2011	April 2011 South Korean Bank Attack	North Korea	Disrupt Nonghyup Bank/ Embarrass South Korea	South Korea	$RCSI_{North\ Korea} = 0.51$ $RCSI_{South\ Korea} = (-0.51)$
2012	Aramco	Iran	Interrupt Aramco Oil & Gas Production	Saudi Arabia/ Aramco	$RCSI_{Iran} = (-0.30)$ $RCSI_{Saudi\ Arabia} = 0.30$
2013	2013 South Korean Bank Attack	North Korea	Disrupt South Korean Banks and Media Companies	South Korea	$RCSI_{North\ Korea} = (-0.33)$ $RCSI_{South\ Korea} = 0.33$

While the case studies provide a limited data set, there are still important lessons that I can draw out of the data. Using these cases, I will examine six elements related to cyberspace superiority. The cases allow me to examine when, where, how, and how long combatants managed to achieve cyberspace superiority and then to attempt to discern why a particular combatant was successful when others were not. Then I can then consider if the possession of cyberspace superiority by a combatant truly did provide a significant advantage for military operations. First, I will look at what the cases can tell us about what conditions are conducive to cyberspace superiority.

Conditions Conducive to Cyberspace Superiority

There are several possible contenders for conditions conducive to cyberspace superiority. Is it the numbers and skill level of the people available to a combatant? Is it the level of intelligence preparation and capability? Is it the resources available to a combatant? Unfortunately, due to the secrecy surrounding national cyberspace capabilities it is very hard to answer these questions definitively, starting with people.

Libicki and others have maintained that the most important resource in cyberspace warfare is highly trained people, but do the case studies support this contention? To answer this question, I would need some method of determining the relative quality of various nations' cyberspace forces. Since little to no information is available at the unclassified level about the relative quality of cyberwarriors, the only methodology available to an analyst is to examine who was more successful in cyberspace and presume their forces were more capable, which sets up circular reasoning and destroys any opportunity for useful analysis.

Another way to approach the problem is to assume that the capability of a nation's cyberspace force is roughly equivalent to their nation's level of cyberspace capability. Unfortunately, this methodology does not stand up to scrutiny. For example, if an analyst were to compare North and South Korea, South Korea has one of the worlds most connected and cyberspace savvy populations measured by Internet connectivity, broadband penetration, and a number of other measures. By any measure, North Korea is one of the world's least connected nations. On the surface, it appears that an analysis of the various cyberspace conflicts between the two might produce some useful information, but there is not a valid correlation between the cyberspace capability of a nation's population, and its cyberspace domain forces. North Korea has placed tremendous emphasis on cyberspace warfare, while South Korea appears to have put relatively less resources and people into cyberspace warfare. Therefore, it does not appear that "success" provides a reliable way to estimate the capabilities of a nation's cyberspace forces since a circular argument seems the only outcome.

Without data on how capable various nations' cyberspace forces are independent from their success, it is impossible to determine if the capability or number of people is an important determinant in achieving cyberspace warfare. In the second area of intelligence, we can draw at least a few qualified conclusions.

In several of the case studies where attackers achieved cyberspace superiority, they successfully prepared their intelligence analysis of the adversary. Analysts have identified that building Stuxnet required significant intelligence preparatory work. In the unsuccessful attacks against Estonia, the Russians had no time for extensive intelligence preparation resulting in little success. In the Russian attacks on Georgia, it appears that

there was significant intelligence preparation and the attacks were far more successful. I can infer successful intelligence preparation in the Georgian attack from the instantaneous timing of the attacks where the attackers hit multiple targets at the same time as the ground invasion. In the various North Korean attacks, the North Koreans did the intelligence preparation they thought was sufficient in preparation for each attack. However, the North Koreans were only successful in half of their attacks. In the Aramco attack, the Iranians did intelligence preparation, but the attack failed, as they did not solve the problem of crossing the air gap defense mechanism.

These cases lead me to conclude that successful intelligence preparation likely contributes to cyberspace superiority, but it does not completely determine who will be successful. A final area to examine is the physical resources available to an attacker.

As I noted earlier, there is no reliable way to compare the relative strength of cyberspace forces in all the cases; however, there are two cases where I can confidently say that one side had more resources committed. In all the North Korean attacks, it is impossible to say with certainty whether North Korean forces committed more resources than South Korea. With Russia and Estonia, it is also not clear who committed more resources in 2007 because the Estonians placed so much emphasis on cyberspace compared to their much larger neighbor, and it is likely that the Russian government relied on proxy "patriotic hackers" without using the state's full capabilities. It is also unclear how many resources the Iranians dedicated relative to the Saudis. The only two cases with a clearly stronger side are with the United States and Israel versus Iran in the Stuxnet case, and with Russia versus Georgia.

In both of the cases with a great disparity in resources and capability, the stronger combatant gained cyberspace superiority. However, the sample size is so small that the only conclusion I can draw is that I do not have any cases where a clearly weaker opponent definitively achieved cyberspace superiority. This finding is unsurprising, but at least allows me to state that I do not have any evidence to disprove the contention that the more capable, more heavily resourced force in cyberspace has an advantage.

This data limitation prevents me from making any firm conclusions about the contribution of physical resources to cyberspace superiority. As more cases of cyberspace conflict occur, it should be possible for researchers to determine the relative importance of the amount of physical resources and infrastructure available to combatants and compare that to other factors such as intelligence preparation. I next turn to analysis of the offense and defense in the case studies.

Offense versus Defense

Despite the predictions of some advocates, the cyberspace "bomber" does not always get through and the offense does not seem to have an overwhelming advantage. Out of eight case studies, the attacker had the cyberspace superiority advantage in four of them and the defender the advantage in the other four. In addition, there were wide differences amongst the cyberspace superiority gained for both attackers and defenders.

There was great variation in the amount of cyberspace superiority gained by combatants on both the offense and the defense. Russia achieved the highest cyberspace superiority of an attacker against Georgia with an $RCSI_{Russia}$ of 0.61, which is probably getting close to the Air Force Doctrine Document (AFDD) 3-12 definition of cyberspace supremacy, as the Georgians had little to no ability to interfere with what the Russians

were doing in cyberspace. The United States and South Korea established the highest cyberspace superiority as a defender with an $RCSI_{US/South\ Korea}$ of 0.46 in 2009. There were also cases where attackers and defenders had very low levels of cyberspace superiority.

This limited data set does not support a strong advantage for either the attacker or defender. The details of the case studies do seem to indicate that if there is an advantage for the offense, it is short lived.

Persistence of Cyberspace Superiority

In seven of the eight cases, the persistence of the attack, and therefore cyberspace superiority, was less than two weeks. This finding has important implications for one of the supporting questions related to my research question, which asked if a state of cyberspace superiority would be persistent once achieved. Clearly, the cases here suggest that it will not be persistent because defenders in most of the cases reacted to defend their systems with increasing success over time.

The one case where the attacker managed significant persistence measured in years was the Stuxnet attack. The Stuxnet attackers accomplished this persistence by carefully designing Stuxnet to keep the attack hidden, and instead to cause the Iranians to blame other issues, such as poor workmanship, for the continuing failure of their centrifuges. Once the Iranians realized that they were under cyberspace attack, they claim they were rapidly able to repair the damage. It is possible that Stuxnet still managed some persistence after discovery due to the way the designers programmed it to hide and re-propagate, but there is no data in the unclassified sources to determine how successful it was at persisting after being discovered. The short persistence of cyberspace

superiority in most of the cases supports the theoretical expectation of short persistence in chapter 3.

There are two tentative lessons that we can draw from this data on persistence. One is that the majority of cyberspace attacks only persist for approximately two weeks or less, and so attackers should plan around a limited timeframe. The second lesson is that if an attacker wants to achieve persistent effects, the only way that an attacker has been able to accomplish that goal is to mask that an attack is occurring at all. An attacker needs to hide the attack and make it appear as if something else is happening if the attack is to persist for an extended timeframe. Once defenders understand that they are under attack, they will react quickly and bring in the resources they need to stop the attack. In the Aramco case, Saudi Arabia quickly brought a team of computer security experts into the country to help stop the attack. Even less cyberspace-capable nations have this option. If something is important enough to attack, it is probably important enough to defend. The local character of the cyberspace superiority achieved in these cases also contributed to its lack of persistence.

Scope of Cyberspace Superiority

In none of the cases did a combatant achieve any significant level of universal cyberspace superiority. There is not even much evidence of a combatant achieving cyberspace superiority in multiple local areas simultaneously. The case that comes closest is that of Russia versus Georgia where the Russians attacked a number of different systems and brought them down over the duration of the conflict, which was admittedly very short. If the conflict had turned into a stalemate in the land domain, would Russia have been able to maintain their cyberspace superiority and expand it? It is impossible to

say with certainty because the Georgians were already seeking outside help to increase their capabilities when the conflict ended. Of course, on the Russian side, the Russian government used proxies, and not their full cyberspace forces. Had the Georgians been successful in bringing in outside help, the Russians had further capabilities they could have brought to bear as well.

The data simply cannot answer the question of the efficacy of universal cyberspace control, because no nation has yet attempted to achieve such superiority. No nation with a significant cyberspace capability has attempted seriously to disrupt the social fabric of a target country over a substantial timeframe. It is even questionable if disruption of a single country or theater of war would be truly universal since a nation can run cyberspace capabilities from servers on the other side of the planet. It is likely that universal cyberspace superiority would have to be world-wide. Although the data does not include attempts to gain universal cyberspace superiority, do the attempts to gain local cyberspace superiority in these cases demonstrate the ability to affect significantly military operations?

Cyberspace Superiority and the Physical Domains

In the Russia versus Georgia case, Russia accrued advantages to their conventional forces they would not have had without the cyberspace attacks. This case is important as the only case in which an attacker used cyberspace operations in conjunction with conventional physical forces. The Russians not only achieved a very high level of cyberspace superiority, they achieved a high level of success in their kinetic campaign. Of course, the Russians had overwhelming superiority in all domains and had planned for the attack and caught the Georgians unprepared for their onslaught.

The disruption of the Georgian communication networks did have a significant effect on the Georgian ability to resist the invasion. Russian forces would likely have conquered Georgia without the cyberspace attacks but the lack of communications prevented the Georgians from mounting a more effective defense. Had the Georgians been able to mount a more effective initial defense it could have given them added time to get the international community involved, and given them more leverage at the conference table. The lack of ability for the Georgian government to get their side of the story out further hampered them, and the Russian strategic information warfare attacks on the Georgian banking system put some pressure on Georgian elites to end the conflict. Russia clearly enjoyed some significant advantages from their cyberspace superiority. There is no definitive evidence of conventional military forces supporting cyberspace attacks from the physical domains in the case studies, but it may have occurred.

Military forces will likely not just receive support from cyberspace; they can provide support to cyberspace forces in conflicts as well. If a special operations soldier infected the notebook computer North Korea used in the April 2011 attack, then it would have been an example of conventional military forces supporting cyberspace warfare. It is not clear if that is what happened, but it could have been the propagation pathway for the cyber weapon. One of the two potential propagation pathways for the Aramco attack also involved physical forces; they likely were Iranian Revolutionary Guard Corps (IRGC) operatives. Military operatives or forces may have propagated Stuxnet at some point as well. What are not included in the case studies are overt physical attacks in support of cyberspace warfare, but combatants should still expect them.

Combatants can improve their cyberspace superiority through physical attacks on cyberspace related resources. The Russians could have done this in the Georgian case as they were accomplishing cyberspace attacks in conjunction with a physical military assault. The fact that they chose not to does not mean it will not happen in the future. The capability was there, but the Russians did not choose to utilize it. There are several possible reasons for the Russian choice including a low priority placed on the cyberspace aspects of the campaign by Russian forces, lack of targeting data on Georgian cyberspace sites, and the low level of capability demonstrated by Russian forces to attack targets deep in Georgian territory. Future cyberspace combatants should prepare for these types of physical attacks, while seeking to use cyberspace to produce advantage for military operations.

Cyberspace Superiority and Significant Advantage for Military Operations

The Russian attacks on Georgia discussed earlier, show one clear example of significant advantage for conventional military operations accruing to a successful cyberspace combatant. Even without large-scale conventional attack, there are other examples as well.

The small level of cyberspace superiority attained by the U.S. and Israel with Stuxnet was able to provide them some significant advantages they could not get from operations in the other domains. In the Stuxnet case, the United States and Israel did not achieve anywhere near the level of cyberspace superiority that Russia did against Georgia, but their superiority lasted for a longer time. As was noted previously, one of the distinguishing characteristics of the Stuxnet attack is the length of time the attackers were able to continue the attack by hiding its existence.

The United States was under increasing pressure by Israel to do something to stop the Iranian nuclear program. The Bush administration did not want kinetically to strike Iran because it felt that a strike would not be effective and would have significant negative consequences across the Middle East.[73] Had the Israelis kinetically attacked Iran, the outcome could have been even worse as the Israelis had less capability and all of the additional political baggage that went with their peculiar situation in the Middle East. Stuxnet was about buying time to allow sanctions and other political initiatives to work before Israel launched a kinetic strike that no one, including the Israelis, wanted at that time.

The level of cyberspace superiority achieved by the United States and Israel, small as it was, proved sufficient to prevent a kinetic strike, as the attackers were able to slow the Iranian program without kinetic weapons. This accomplishment was a major achievement with significant consequences at the policy level. The next attack had less impact on the policy level, but was significant on the operational level.

Another case where a cyberspace combatant gained significant advantage for military operations through cyberspace superiority was the 2011 bank attack by North Korea. The attack was limited in scale, as the North Koreans only attacked one bank, but it was far more successful in its impact than previous North Korean attacks. The North Koreans managed to dominate the South Korean media cycle, cut 30 million South

[73] Sanger, *Confront and Conceal*, 190.

Koreans off from making financial transactions, and seriously embarrass the South Korean government, all while being able to claim that they had nothing to do with it.[74]

This situation represented significant advantage in military operations for the North Koreans, as it gave them a very low risk way to attack their enemies not available in the other domains. Had the North Koreans used special operations forces or aircraft physically to attack the bank and did the same level of damage, the North Koreans would have come under tremendous pressure from the international community. Instead, the North Koreans were able to deny they had anything to do with the attack, which gave their allies such as China the ability to block any proposed diplomatic action against them. Each of these cases shows significant advantage that accrued to the attacker due to his achievement of cyberspace superiority.

Even from the limited cases we have available, it can be seen that higher levels of cyberspace superiority correlate to advantage in military operations. This evidence supports the hypothesis that cyberspace superiority creates a significant advantage for military operations. Yet, due to the shortage of cases and the ambiguity of the evidence available, it is not possible from just these cases to say with certainty that cyberspace superiority creates a significant advantage for all military operations. However, when connected to the theory behind cyberspace superiority as presented in chapters 2-4, there is strong evidence to suggest that indeed cyberspace superiority, when effectively achieved by a protagonist, does create a significant advantage. In the final chapter, I will

[74] Ryan Mauro, "Major North Korean Cyber Attack on South," *Frontpage Mag*, 1 September 2011. http://frontpagemag.com/2011/ryan-mauro/major-north-korean-cyber-attack-on-south/.

compare the evidence to my hypotheses and examine the conclusions that result from this study.

CONCLUSIONS

The existence of cyberspace superiority has important implications for warfare in the 21st Century. Without an understanding of the framework underlying conflict in cyberspace, nation-states will be less successful than they could be in utilizing and exploiting this new domain. Cyberspace superiority, with its linkages between local and universal, connections between means and ways, blocks by enemy combatants, and the continuing dynamic of struggle provides such an organizing framework. Combatants can measure cyberspace superiority, analyze it, and use it for planning. In the end, cyberspace combatants should utilize cyberspace superiority as a concept for the simple reason that it is useful, and can lead to better outcomes in warfare.

Unfortunately, there has been little academic work done on cyberspace superiority. Many authors have dismissed it too quickly as unattainable, largely because they did not make a distinction between universal cyberspace superiority and local cyberspace superiority. While global "command of the cyber" may be unobtainable, varying levels of cyberspace superiority are possible in specific local areas of cyberspace with enough persistence to accomplish a combatant's objectives. Cyberspace superiority is useful as a concept because it can help to focus and connect a combatant's efforts in cyberspace.

To build an understanding of what constitutes superiority in cyberspace, it is necessary to start with an understanding of what constitutes cyberspace. Cyberspace is a domain created by the connections between computing devices. The Joint Staff has defined cyberspace as, "a global domain within the information environment consisting

of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[1]

Within cyberspace, combatants seek to connect their means and ways, while at the same time their adversary is attempting to block them from achieving their objectives. A defender can interfere with an attacker's means or ways, and an attacker in turn can attempt to interfere with the defender's blocks. Out of this dynamic comes the contest for cyberspace superiority that I illustrate below in figure 15.

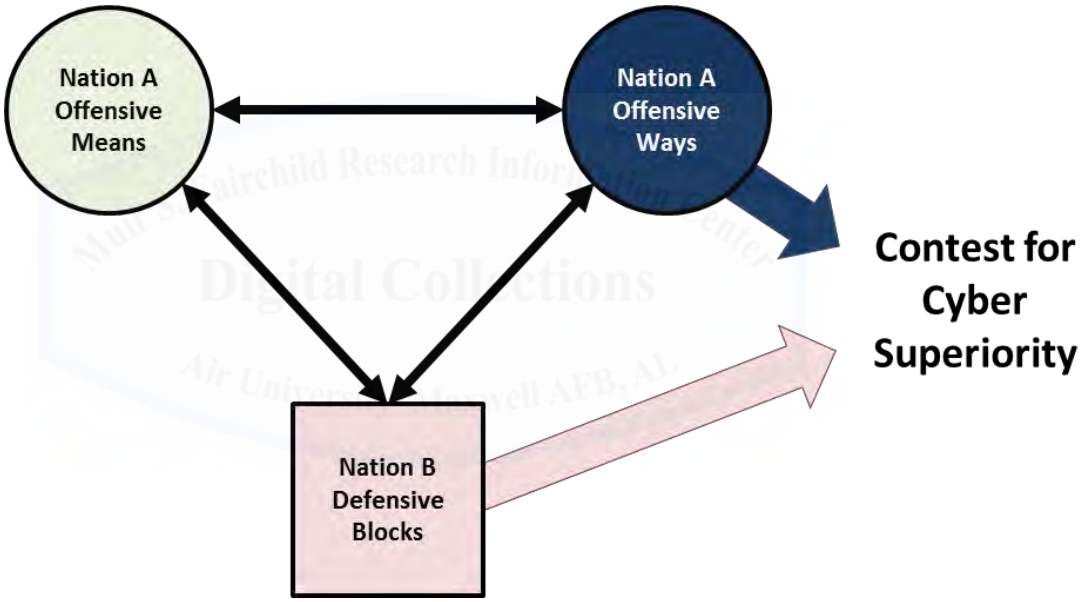

Figure 15 – Cyberspace Conflict
Source: Author's Original Work

This simplistic illustration can be fleshed out by including what tools combatants use in these various categories. When the tools are included, I depict an illustration of the cyberspace conflict system in figure 16.

[1] Joint Chiefs of Staff, Joint Operations, Vol. 3-13, *Information Operations*, 2012.

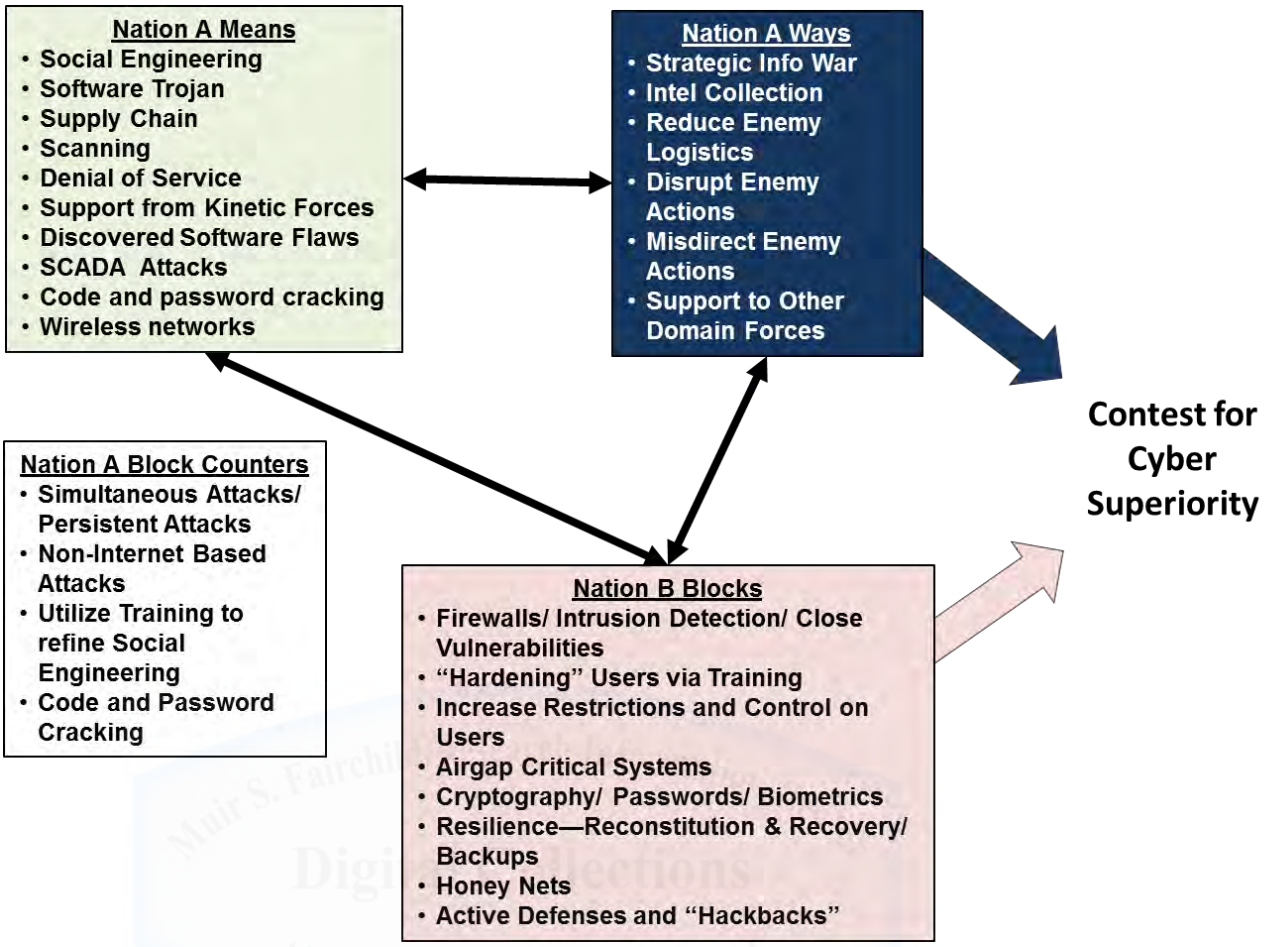

Figure 16 – Detailed Cyberspace Conflict Diagram with Tools and Ways
Source: Author's Original Work

A description of all these cyberspace means, ways, blocks and counter-blocks is included in appendix C. Note that the attacker aims some of his tools at mitigating or disrupting the defender's attempts to stop him, instead of directly at achieving cyberspace objectives.

Cyberspace superiority is fundamentally about achieving enough control of the cyberspace domain to enable the successful completion of your objectives, while blocking your enemy from accomplishing his objectives. Domain specific forces always attempt to control their domains, as they have to establish some minimal level of control

to operate effectively.[2] Cyberspace operators are no different, nor should they be. According to Air Force Doctrine Document (AFDD) 3-12, cyberspace superiority is, "The operational advantage in, through, and from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference."[3] This is a clear and useful definition, which leads to my research question.

The heart of this project was whether a meaningful level of cyberspace superiority was achievable and would provide a significant advantage in military operations.

Research Question: Does a nation that achieves a level of cyberspace superiority during a conflict gain a significant operational advantage?

This question brought up several supporting questions that I had to answer in this work. First, is cyberspace superiority a local or universal concept? In other words, does cyberspace superiority apply only in small areas or across entire theaters? The second question dealt with the issue of persistency with regard to cyberspace superiority. Once gained, was cyberspace superiority likely to last for years, months, weeks, or minutes? The third supporting question sought to determine if analysts could reliably measure cyberspace superiority. Without an analytically sound and repeatable method of measuring cyberspace superiority, its presence could become merely a matter of opinion not useful for rigorous analysis.

In the other domains of land, maritime, and air, domain superiority provides significant advantage for military operations. Despite its unique characteristics as a

[2] Thomas David McCarthy, "Traveling Domain Theory: A Comparative Approach for Cyberspace Theory Development" (PhD diss., Fletcher School of Law and Diplomacy, 2012), 188.
[3] Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations. Change 1*, 15 July 2010, 2.

domain, my hypothesis was that cyberspace will also provide a similar advantage. My hypothesis was,

> **Research Hypothesis: If a nation achieves cyberspace superiority during a conflict, then it gains a significant operational advantage.**

To model more clearly the variables in my hypothesis, I turned to Stephen Van Evera's political science theory methodology. Utilizing his definitions of variable types, my research hypothesis is in figure 17.

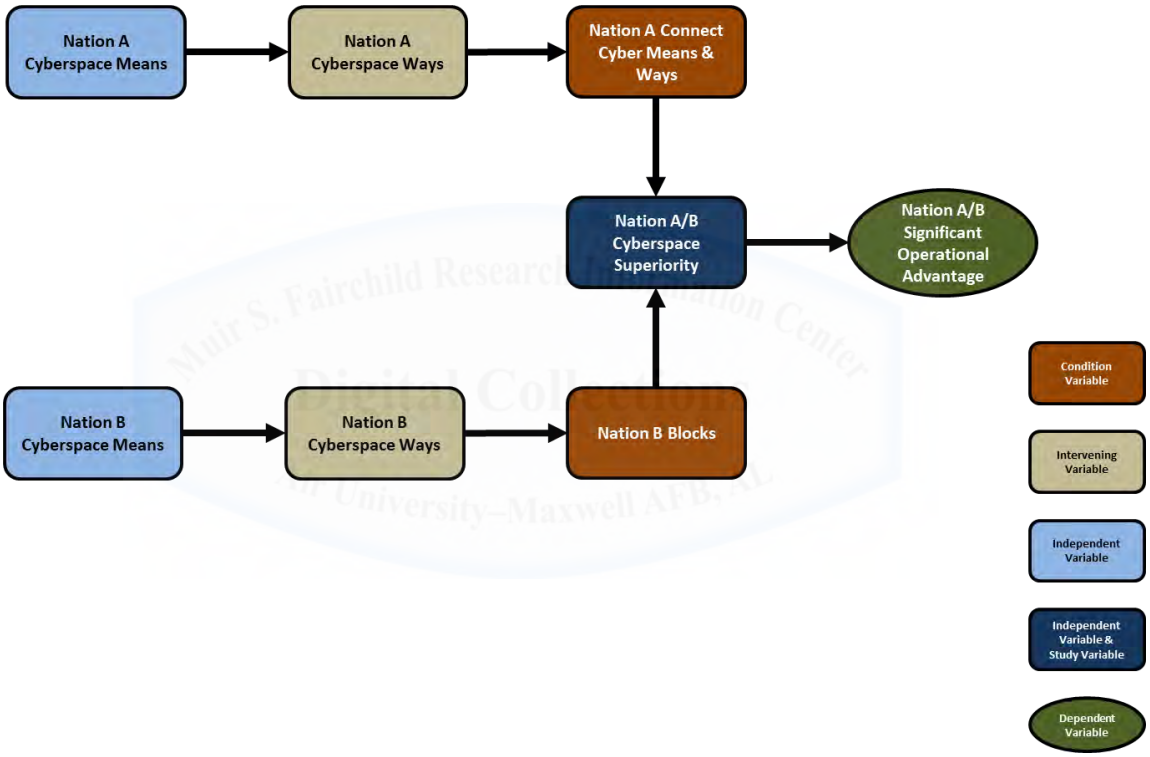

Figure 17 – Research Hypothesis
Source: Author's Original Work

Cyberspace superiority is the independent study variable, and it is influenced by the two condition variables of connecting cyberspace means and ways and the defender's blocks. Significant operational advantage is the dependent variable that I was looking for in this

study and either the attacker or defender can attain it depending on how successful they are in achieving cyberspace superiority.

To fill in these variables and test my hypothesis, I first examined superiority concepts in the land, maritime, and air domains. Next I built a weighted preference model that allowed me to do qualitative analysis on the eight available case studies that met my research criteria. Finally, I did qualitative analysis on three case studies to validate the model and help draw out the conclusions for this study. To lay the foundation, I first turned to the other domains to see what elements of domain superiority I could usefully apply to cyberspace.

Elements of Domain Superiority

Combatants have fought in each of the other domains almost as soon as mankind figured out how to operate within each domain. Humans have sought superiority on the land, in the maritime domain, air domain, space domain, and cyberspace domain. I excluded space from this analysis, as there is not yet a consensus on how domain superiority operates in space, or enough case studies for an analyst to examine.

One of the important elements that came out of my survey of domain superiority in the other domains is the importance of the universal versus local levels of superiority and their interactions. Each domain was different in this regard with some like the maritime domain placing more importance at the universal level, and others like the cyberspace domain placing more importance at the local level. A lack of clarity on whether the superiority under discussion is at the universal or local level generates much

of the confusion that results when analysts argue past each other about domain superiority.

The universal and local levels of superiority interact in all of the domains and do not stand separate. In most of the domains, this interaction occurs in the same two ways. First, combatants generate the forces that fight at the local level at the universal level before moving those resources to the appropriate local area. Second, the losses sustained by those combatants in conflict reduce the forces available at the universal level. That reduction then impacts what forces a combatant has available to allocate amongst all the local areas. In cyberspace, combatants still generate resources at the universal level before pushing them to local areas, but the feedback mechanism is different. In cyberspace, losses do not normally occur via physical destruction such as an attacker sinking a ship or shooting down an aircraft; instead, they occur when the enemy learns how to defeat the tools and weapons used by a cyberspace combatant. The feedback produced has a similar outcome, but there is a different mechanism behind it.

Another difference in the operation of domain superiority across the domains is the amount of overlap between the offensive and defensive sides of superiority. In some domains, such as the maritime domain, most forces can operate well on both the offensive and defensive. In the air domain, there is a mixture with some forces able to undertake offensive or defensive missions. In the cyberspace domain however, tools and weapons are normally very specific and combatants cannot shift them from offense to defense or vice versa, which reduces their flexibility. I wove both the offensive/defensive split, and the universal/local separation throughout all of my analysis of the elements of domain superiority.

In my analysis of each of the domains, I looked at six different areas. I examined the domain's geography and characteristics, offensive or defensive primacy, the method of gaining domain superiority, the use of domain superiority, the persistence of domain superiority, and measurement concepts of superiority in the domain. I will follow the same pattern as I pull out the most important elements from all of the domains.

Geography and Characteristics of the Domains related to Superiority

The land domain is the one most unlike the cyberspace domain. Physical features such as mountains and rivers dominate the land domain and as a result, geography dominates superiority in the land domain. This normally produces a sequential approach to land domain superiority since land-based forces generally have to protect their lines of communication and must move sequentially towards their objectives. The maritime domain shares more characteristics with the cyberspace domain than the land domain.

The maritime domain consists of a bounded maneuver space accessed by technology that is principally important due to the sea lines of communication that carry most of the world's cargo. Like the land domain, the maritime domain has distinct edges with the other domains; however, unlike land, the maritime domain produces its most significant effects in the other domains. The interaction of the land domain with the maritime domain produces a large number of chokepoints that are important strategic terrain in the maritime domain. These chokepoints have similarity to cyberspace chokepoints and produce some similar effects. Another similarity with the cyberspace domain is that the maritime domain is vast and open and humans do not live there, so normally no one has superiority in most of the maritime domain; it is "uncommanded."

Combatants access the maritime domain through technology and expensive infrastructure such as ships and ports. In this way, the maritime domain is similar to the air domain.

The geography of the air domain is very different from that of land or sea and gives the domain its unique characteristics, including that the air domain is mostly open and less constrained. The air domain differs from the land and maritime domains in that air domain forces can more easily bypass defenses to target directly civilians and infrastructure, which can make air domain warfare much less sequential. The great speed, long range, and flexibility of modern aircraft also make it very easy for air domain forces to concentrate rapidly on a mission or location. Combatants access the air domain through technology much as combatants access the maritime, space, and cyberspace domains. While still very distinct, a combination of characteristics from the air and maritime domains apply to the cyberspace domain.

The fact that cyberspace is man-made, but connected to the physical world drives the geography of cyberspace. There are chokepoints in cyberspace that we can consider as roughly analogous to mountain ranges or other features in the land domain, but cyberspace operators create them and they can be rapidly changed, moved, or entirely deleted. This mutability has significant implications for cyberspace superiority and the continuing rapid improvement of hardware across cyberspace further accentuates this constant mutability. As cyberspace grows and expands, its network structure gives it a high level of built-in resiliency to attacks. As hardware improves, the cost of entry into cyberspace continues to decrease.

An entry-level capability for a nation-state in cyberspace can be very economical; however, significant capability is expensive. It seems counter intuitive for a domain that

derives its very existence from technology, but well trained and capable people are more important in the battle for cyberspace superiority than equipment. However, even the largest cyberspace forces are miniscule compared to the vastness of cyberspace and so, like the maritime domain, normally no nation will have cyberspace superiority in an area of cyberspace. Part of the reason for this characteristic is the specialization of cyberspace weapons that cannot simply seek out and destroy enemy forces autonomously.

Offensive cyberspace weapons have no ability to detect enemy offensive cyberspace weapons and so they cannot destroy them in opportune "meeting engagements." This makes cyberspace forces very different from land, maritime, or air forces who can all detect and react to the unexpected presence of enemy forces. In this respect cyberspace forces are most like the satellites of the space domain that fly past each other while continuing to do their individual missions unless specifically instructed to do something else. An area of great divergence among the domains is whether the offensive or defensive has primacy in the domain.

Offensive or Defensive Primacy in the Domains

Colin Gray has identified that the advantage for offense or defense in a given domain is dependent upon the "tactical-technical logic" of that domain.[4] Thus, the advantage can shift within a given domain due to changes in either tactics or technology, but the advantage does not normally shift rapidly.

In the land domain, the defensive currently has the advantage in the tactical-technical logic. The reason for the advantage of the defender is that normally, the

[4] Colin S. Gray, *Modern Strategy* (Oxford: Oxford University Press, 1999), 110.

defender can remain hidden and under cover, while the attacker has to move forward in the open and exposed. This situation is what accounts for the military maxim that an attacker should outnumber the defender three to one if he is going to be successful.

In the maritime domain, neither the offensive or defensive has clear primacy; it depends on the specifics of the engagement. This is because, unlike the land domain, generally in maritime surface warfare the attacker and defender can see each other at the same time and have an equal opportunity to fire first. There are several exceptions to this general rule, in undersea combat, the advantage goes to the one who stays hidden, which gives a benefit to the defense as it is easier to stay silent and hidden while remaining in place. In addition, a fleet operating within range of friendly land based defenses gains a significant advantage over an attacking fleet. Like the maritime domain, the air domain also does not have clear primacy for the attacker or defender.

While earlier air domain theorists favored the offensive, whether the defensive or offensive had primacy in the air domain has shifted over time with technological change. Right now, there is no clear primacy to the offense or defense; the more effective operational and tactical force is likely to defeat its foe on either the offense or defense. The Israeli Air Force has demonstrated the importance of this factor by defeating its foes whether on the offensive or defensive through superiority in equipment, tactics, and strategy.

The advantage in the cyberspace domain, however, goes to the attacker who can be proactive, as he can remain hidden and anonymous, while the defender is out in the open and reactive. In the land domain, attackers have to unmask to attack; in the cyberspace domain it is the defenders who are out in the open, and it is the attackers who

have the advantage of stealth. Offensive cyberspace weapons striking the inside of an enemy system attack in a two-stage process, first they gain access, and then they execute the mission. Most cyberspace weapons rely on deception to get in, and stealth to persist and accomplish their missions, which means defenders will generally be unable to see them coming and gives an advantage to the offense. This advantage is not strong enough to overwhelm other factors, and the defense can be, and often is, successful in gaining and maintaining superiority in cyberspace.

Method of Gaining Domain Superiority

There is great variation amongst the various domains in how a combatant attains domain superiority. One reason for this difference is that in each of the domains the importance of the local and universal levels of superiority changes. In the land domain, there is a balance between the local and universal levels.

Physical presence is the key to establishing land domain superiority but it is not sufficient; a combatant also needs population acceptance to make his superiority secure. For the United States, establishing physical presence has been easier than population acceptance in the last few conflicts. Successful combatants have most often established physical presence by defeating the enemy army in battle and occupying his territory. Combatants can also gain control through some form of negotiated settlement or peace treaty that transfers land from one combatant to another. In the maritime domain, there are several competing theories about how to gain superiority.

Maritime theorists have disagreed on the relative importance of the local or universal level in gaining maritime superiority. For Mahan, the only way to gain maritime superiority was to destroy the enemy's fleet, while Corbett saw other

possibilities. For Corbett, combatants could establish a form of maritime superiority via a blockade, or commerce warfare and avoiding the enemy fleet completely. The reason behind these different theories of gaining superiority is that Mahan saw maritime superiority as universal and Corbett saw it as local. The air domain is a mixture of both universal and local.

The universal level of air superiority is more significant than the local level due to the excellent mobility of airpower, the concentrated character of the airpower instrument and the vulnerability of universal airpower to attack. To gain air domain superiority at the universal level a combatant needs to attack the enemy's offensive and defensive air domain forces. An enemy can normally shift forces in the air domain rapidly so defeating all the forces in one local area may not bring sustained advantage if the enemy can simply shift forces from another area to fight for the same local area again. Local air superiority involves defeating only those enemy forces required to attain a specific objective in a local area whether that objective is offensive or defensive. This local superiority may be all that is required if the objectives sought by a combatant are limited. For cyberspace combatants, local superiority will normally be all that is achievable.

One method of achieving a form of universal cyberspace superiority would be to focus on chokepoints to control the flow of information and degrade the enemy's ability to use cyberspace, but at the current time, policy and technical limitations make successfully controlling all chokepoints in cyberspace unlikely. The network design of cyberspace enables most traffic seamlessly and rapidly to divert around attempted blocks with no active intervention by the user. Also, because of the problems with attribution, it

will not be clear to a combatant, which streams of information belong to the enemy. In addition, the enormous amount of data passing across chokepoints such as major undersea cables makes filtering it very difficult with current technology. Since controlling chokepoints is not practical with the current technology and structure of cyberspace, combatants should pursue whatever universal superiority is attainable, while focusing on the fight for local cyberspace superiority.

In cyberspace, the local level of superiority is far more important than the universal when compared to the other domains. There are a number of reasons for this situation. First, it is difficult to move cyberspace weapons from one local area to another. Second, offensive and defensive forces in cyberspace are very different, which prevents combatants from moving them between offensive and defensive missions. Next, attackers design specialized cyberspace weapons, which typically affect a single system. A final reason why cyberspace superiority tends to be local is that it is extremely difficult for combatants to find and attack enemy cyberspace "fleets" and "armies." These factors suggest that combatants should focus on gaining local cyberspace superiority.

An attacker will gain local cyberspace superiority by successfully accessing enemy systems to accomplish desired objectives, while a defender will gain local cyberspace superiority by successfully blocking the attacker from achieving his offensive objectives, and protecting friendly access to cyberspace systems. The constant maneuvering between attackers and defenders sets up a dynamic in cyberspace akin to Clausewitz's wrestlers as the maneuvers of each side affect the options available to the other. Once a combatant has gained a measure of domain superiority, what can combatants do with it?

Use of Domain Superiority

As we saw in the gaining of domain superiority, the use of superiority across the different domains varies. At its heart, the use of domain superiority is about a combatant accomplishing the goals and objectives he or she has set in that domain. In the land domain, combatants often connect these objectives to the purpose of the conflict.

Once a combatant establishes superiority in the land domain to include the acceptance of the situation by the population, he can normally dictate terms to the enemy. If the conflict continues in other theaters, a combatant can utilize the portion where the combatant has superiority to produce resources and continue to pursue overall victory. World War II provides numerous examples of utilizing conquered terrain to produce the resources needed to continue the war. In the maritime domain, combatants most often utilize superiority to protect sea lines of communication.

Once a combatant gains maritime superiority, he or she can protect friendly sea lines of communication and attack those of the enemy, while enabling friendly power projection ashore and preventing enemy power projection. Some theorists, such as Mahan, viewed maritime superiority as critical to a nation because of its potential control of commerce. Corbett agreed that seaborne commerce was vital, but he also saw the importance of being able to utilize the maritime sphere to influence the land domain. Since the maritime domain cannot be owned in the same manner as the land domain, Corbett saw that the principal contribution of maritime superiority was to influence the land domain through sea lines of communication or power projection ashore. While there are lines of communication in the air domain as well, combatants normally focus the use of superiority on the accomplishment of objectives.

There are three major ways that airpower analysts have suggested a combatant can use air superiority to achieve campaign objectives. The first is to attack the enemy population to put pressure on enemy decision makers. The second is to attack infrastructure or industry to prevent the enemy from constructing weapons, and the third is to use airpower to support surface forces. This support to surface forces can include attacking enemy forces engaged in combat with friendly forces, attacking enemy forces in reserve, and resupply of friendly forces. Combatants have utilized all three approaches at various times in the air domain; they are not mutually exclusive and often reinforce each other. For example, bomber attacks on railway targets in France prior to the Normandy invasion affected the German war economy and prevented the rapid transfer of troops to the front. While these approaches can be combined, punishment of enemy populations has normally not produced decisive results and I agree with Robert Pape that normally the best approach is to attack the enemy's military strategy.[5] If the enemy is attempting to achieve his objectives with his army, this will often take the form of attacking the enemy army. In cyberspace, like the air domain, combatants focus their use of superiority on the accomplishment of their objectives.

There are three main ways that cyberspace combatants utilize the superiority they gain; the first is strategic information warfare. Strategic information warfare is when a combatant reaches directly through cyberspace to affect enemy targets and systems. Examples include taking down a power grid, disrupting communications, or attacking any computer driven device or process. For coercion via strategic information warfare to

[5] Robert Pape, *Bombing to Win: Air Power and Coercion in War* (London: Cornell University Press, 1996), 15.

succeed, the cyberspace attacks must be more unpleasant than the sacrifice the attacker is asking the defender to make. It also needs to appear that the effects of the attacks are going to get worse, which is difficult to achieve in cyberspace due to the tendency of offensive weapons rapidly to lose their effectiveness.

The second way that a combatant can utilize their cyberspace superiority is as an enabler and integrator of other domain forces. Often, cyberspace forces' most important offensive contribution in a conflict will be as an enabler of forces in the other domains. Cyberspace superiority can enable success in the other domains by providing the collaborative planning and communications tools modern combatants utilize as well as confusing and blinding enemy forces, whose vulnerability to these attacks will depend on the extent that they rely on cyberspace. Cyberspace superiority can also enable crucial intelligence work that can contribute to the success of physical domain forces.

The third, and perhaps most important thing that a combatant can do with cyberspace superiority, is to protect his systems. This protection is especially important for a highly connected nation like the United States with cyberspace enabled military forces. U.S. forces have become increasingly reliant upon cyberspace-enabled tools and connectivity such as friendly tracking systems, Remotely Piloted Vehicles (RPVs), and data links. On the home front, the loss of cyberspace superiority would open up the nation's infrastructure to potential attack from other nations' strategic information warfare. Once a combatant gains and uses domain superiority, the next question is how long he can hold it.

Persistence of Domain Superiority

The persistence of domain superiority varies widely with land superiority being the most persistent and cyberspace superiority the least. The characteristics of the various domains and the timescales associated with action within them drive these differences.

Land domain superiority tends to be persistent due to greater influence of the universal level of superiority as well as the sequential tendencies of land combat, the inertia of populations whose support changes slowly, and the current primacy of the defensive. All of these factors combine to make changing land superiority very difficult. Persistence of superiority in the maritime domain is more variable.

Whether the maritime superiority gained is local or universal will greatly affect the persistence of maritime superiority. According to Mahan, who focused on universal maritime superiority, superiority should be persistent based on major fleet actions that would affect universal superiority. If the enemy refuses to fight a major fleet action for universal control, then control will not only be localized, but also fleeting as the enemy can dash out of port to raid convoys and establish local control in an area, but then retreat back into port when threatened by the main adversary fleet. Persistence in the air domain is similar to the maritime domain with long persistence only available with universal air superiority.

Because of the high mobility of air domain forces to move from one local area to another, a combatant will be able to achieve persistence of superiority in the air domain only if he is able to achieve universal versus local air superiority. Airpower theorists, who saw that air superiority could be local, also recognized that local superiority would

tend to be transient. Air superiority will tend to be local and transient unless one side has such an overwhelming abundance of superiority that they can achieve across the entire theater of operations as the Coalition did in the 1991 Gulf War. Unfortunately for cyberspace operators, they normally can only achieve local domain superiority, which also limits them to short persistence of that superiority.

The persistence of cyberspace superiority will generally be very short due to the replicability of cyberspace, its great speed of action, and the rapid degradation of offensive cyberspace weapons once defenders discover them. Software and data in cyberspace are replicable, which makes software and data based attacks easier to recover from quickly. The short timescales of cyberspace produce great speed of action and rapidly changing dominance, which reduces persistence. Another reason why cyberspace superiority will not tend to be persistent is the rapid degradation in the effectiveness of offensive cyberspace weapons once defenders discover them. Once a defender finds an enemy weapon, the defender will be able to inoculate his or her other systems and the weapon will lose most of its utility for future attacks. To verify any of these findings against real world case studies, analysts have to have some reliable methodology to measure domain superiority, which is where we turn next.

Measurement Concepts of Domain Superiority

Because there is such breadth in the characteristics of domain superiority across the domains, there is also great variation in how it is measured. Several of the domains though, have elements of measurement that have great utility in cyberspace.

Land domain superiority consists of territorial control and acceptance of that control; analysts use a range of metrics to measure territorial control by which

combatant's soldiers occupy terrain and control. Determining whose soldiers occupy which portion of the contested terrain is by far the easier task. James Clancy and Chuck Crossett identify three main types of population control metrics they label measures of sustainability, legitimacy, and stability.[6] Analysts can think of sustainability as supply and resources getting to the insurgent enemy, legitimacy focuses on the effectiveness of the friendly government in the eyes of the population, and stability measures the level of security and ability to function of a local society. Measuring maritime domain superiority requires a very different set of tools.

Measures of maritime superiority include the balance of forces between the two fleets, metrics to measure the openness of sea lines of communication, and the ability of combatants to project power from the maritime environment into other domains. Metrics to compare fleets should focus on combat effectiveness, which can be difficult to measure. Simple comparisons of tonnage or types of ships will likely be inadequate. Metrics that measure how much friendly shipping is reaching its destination and how much enemy shipping is not, will provide a picture of how open the sea lines of communication are. Finally, if a maritime combatant can utilize the maritime environment to project power into the air or land domains at will through amphibious assaults or carrier borne aviation, it demonstrates a high level of maritime superiority. Like the maritime domain, the ability of cyberspace to project power into the other domains will be a key component of measurement, but the air domain measurement techniques have more applicability.

---

[6] James Clancy and Chuck Crossett, "Measuring Effectiveness in Irregular Warfare," *Parameters*, Summer 2007, 96.

Measuring air domain superiority is a question of assessing how effectively an attacker or defender is accomplishing his or her objectives in the domain. Common indicators include how often strike aircraft have to jettison their bombs before getting to their targets, how often targets are struck successfully, how many enemy sorties get into friendly territory, and what their effectiveness was. Many of the indicators used in the air domain such as strike effectiveness and number of successful enemy air attacks transfer readily into the cyberspace domain. Like with air domain superiority, cyberspace superiority measurement will also focus on a combatant's achievement of objectives, both on the offensive and defensive sides.

Cyberspace domain superiority is fundamentally about a combatant being able to achieve his objectives in cyberspace while preventing the enemy from achieving his objectives, thus both combatant's objectives will be key to measurement. On the offensive side, an analyst can best accomplish this by measuring the attacker's success against whatever objectives he was pursuing. On the defensive side, an analyst can measure success by examining the level of functionality of critical systems under cyberspace attack. The most effective way to combine and properly weight these multiple objectives and inputs is through a weighted preference model. Before moving on to that model, a summary of domain superiority characteristics is next in table 12.

Table 12 – Summary of Domain Characteristics and Domain Superiority

Geography and Characteristics	
Land	□ Physical terrain such as mountains, rivers, and swamps dictate lines of communication and which forces are most effective where □ Combat tends to be sequential with forces excluding each other from areas of their control while protecting their own lines of communication

Maritime	• Maneuver space is bounded by land masses and ports which form chokepoints • Sea lines of communication are the key element worth fighting over • Accessed via expensive technology (ships) and expensive entry points (ports)
Air	• Open and relatively unbounded without natural chokepoints • No clear front line involves civilians directly in combat operations • Characterized by great speed of action • Dependent upon technology for access • Accessed via expensive technology (aircraft) and expensive entry points (airfields) • Dominance in this domain is not sufficient for victory, it enables the land and maritime domains
Cyberspace	• Manmade but connected to the physical world • Can usefully be modeled by Libicki's three layers of physical, syntactic, and semantic • An entry-level capability for a nation-state in cyberspace can be very economical; however, significant capability is still expensive • The network structure of cyberspace gives it a high level of built-in resiliency to attacks that focus on interfering with communication between nodes • There are chokepoints in cyberspace that we can consider as roughly analogous to mountain ranges or other features in the land domain • There are two facets to cyberspace's changing geography over time, the first is that combatants can connect, disconnect, or change the linkages between the components that create cyberspace • The second facet of cyberspace's changing geography is that designers continue rapidly to make the individual hardware more capable • Because of the small number of cyberspace forces in relation to the vast amount of cyberspace, normally no nation state will have superiority in a given area of cyberspace • Combatants may restrain themselves in cyberspace to avoid crossing perceived global norms of cyberspace as a global common • Offensive cyberspace weapons have no ability to "see" and react to each other, thus there is no analog to a meeting engagement in

	cyberspace
Offensive or Defensive Primacy	
Land	With modern weapons the defensive has primacy as the defender can stay under cover while the offender must unmask to advance
Maritime	There is no clear offensive or defensive primacy in the maritime domain o Normally both offensive and defensive forces can see each other at the same distance o Exceptions include submarine warfare which favors the offender and a fleet in a defended port which favors the defense
Air	Older theorists favored offensive, advantage has shifted back and forth over time depending on technology
Cyberspace	The advantage in the cyberspace domain goes to the attacker who can be proactive as he can remain hidden and anonymous, while the defender is out in the open and reactive
Method of Gaining Superiority	
Land	Universal – Defeat enemy army to allow physical access to the terrain and then gain control and support of the population Local – Defeat local regular or insurgent forces
Maritime	Universal – Defeat enemy fleet or blockade them in port; weaker combatant can contest by keeping a "fleet in being" and executing small counter attacks Local – Disrupt enemy shipping while protecting your own
Air	Offensive universal – Degrade enemy strategic IADS Defensive universal – Degrade enemy offensive airpower Offensive local – Defeat enemy local IADS Defensive Local – Defeat enemy local offensive airpower
Cyberspace	Controlling chokepoints is one way of establishing universal cyberspace superiority, however it will normally not be possible There are a number of reasons why local cyberspace superiority will normally be all that is achievable o It is difficult to move cyberspace weapons from one local area to another o Offensive and defensive forces in cyberspace are very different, which prevents combatants from moving them between offensive and defensive missions o The specialization of cyberspace weapons that attackers design for a single system o It is extremely difficult for combatants to find and attack enemy cyberspace "fleets" and "armies" An attacker will gain local cyberspace superiority by successfully

	accessing enemy systems to accomplish desired objectives • A defender will gain local cyberspace superiority by successfully blocking the enemy from achieving his offensive objectives, and protecting friendly access to cyberspace systems
Use of Superiority	
Land	• Often control of the land domain will terminate the conflict; if not, combatant can extract resources for continued combat in other areas and domains
Maritime	• Enable shipment of military and commercial goods • Project power into the land domain while preventing the enemy from doing the same
Air	• Offensive – Directly striking enemy centers of gravity to either affect enemy capabilities or change enemy decisions; Support other domain forces • Defensive – Prevent enemy from striking friendly centers of gravity
Cyberspace	• There are three principal methods for combatants to utilize cyberspace superiority o Strategic information warfare: creating direct effects through cyberspace o Enabling other domain forces: utilizing cyberspace to increase the effectiveness of land, maritime, air, and space domain forces o Protecting friendly systems: maintaining the effectiveness of friendly cyberspace systems
Persistence	
Land	• Land domain superiority tends to be persistent due to greater influence of the universal level of superiority as well as the sequential tendencies of land combat, the inertia of populations whose support changes slowly, and the current primacy of the defensive
Maritime	• Whether the maritime superiority gained is local or universal will greatly affect the persistence of maritime superiority o If a combatant can achieve universal maritime superiority through defeating the enemy fleet, then persistence can be high o If the enemy refuses to fight a major fleet action for universal control, then control will not only be localized, but also fleeting as the enemy can dash out of port to raid convoys and establish local control in an area, but then retreat back into port when threatened by the main adversary fleet
Air	• Because of the high mobility of air domain forces to move from one local area to another, a combatant will be able to achieve

	persistence of superiority in the air domain only if he is able to achieve universal versus local air superiority
Cyberspace	The persistence of cyberspace superiority will generally be very short due to the replicability of cyberspace, its great speed of action, and the rapid degradation of offensive cyberspace weapons once defenders discover them
Measurement Concept	
Land	Whose soldiers are in possession of the terrain Metrics to determine the level of support of the population
Maritime	Universal – Remaining capability of enemy fleet Local – Metrics to measure friendly and enemy utilization of sea lines of communication; Ability to project power into other domains
Air	Ability to achieve objectives in the air Relative measurement and trends of resources
Cyberspace	Offensive success is measured by summing the level of objective achievement Defensive success is measured by summing the level of functionality of key systems and the prevention of enemy success

Measuring Cyberspace Superiority

Measuring cyberspace superiority involves both the offensive and defensive aspects of warfare in cyberspace. To measure offensive cyberspace superiority, I multiplied the success an attacker had in accomplishing an objective (S) with the importance or weight of that objective (W) and summed across all of the attackers objectives from 1 to n. This equation defined the attackers OCSI or Offensive Cyberspace Superiority Index.

$$OCSI = \sum_{k=1}^{n} S_k \times W_k$$

On the defensive side, the calculation was similar with the level of functionality of friendly systems (L) replacing S and the criticality of those systems (C) replacing W. The result is DCSI or the Defensive Cyberspace Superiority Index.

$$DCSI = \sum_{k=1}^{n} L_k \times C_k$$

I then introduced reliance on cyberspace (R) to account for differences between combatants in how important cyberspace is to their society. R varies from 0.00 to 1.00 with 1.00 representing complete reliance upon cyberspace. I multiplied the offensive index by the defender's reliance on the cyberspace domain while I multiplied the defensive index by the offender's reliance. This cross multiplication is because the importance of success in the offensive domain depends on how reliant the defender is on cyberspace, while the importance of success at achieving cyberspace superiority in the defensive domain also depends on how reliant the defender is on cyberspace. I therefore calculate the Cyberspace Superiority Index (CSI) for nation A in the following equation.

$$CSI_A = \left((OCSI_A \times R_B) + (DCSI_A \times R_A)\right)$$

Since superiority is relative, what really matters in a conflict is the relationship between the two nations' CSIs. This relative measurement is the Relative Cyberspace Superiority Index (RCSI). For nation A, it is calculated simply by subtracting nation B's CSI.

$$RCSI_A = CSI_A - CSI_B$$

Substituting in all the terms, the total calculation is therefore,

$$RCSI_A = \left(\left(\left[\sum_{k=1}^{n} S_k \times W_k\right]_A \times R_B\right) + \left(\left[\sum_{k=1}^{n} L_k \times C_k\right]_A \times R_A\right)\right)$$

$$- \left(\left(\left[\sum_{k=1}^{n} S_k \times W_k\right]_B \times R_A\right) + \left(\left[\sum_{k=1}^{n} L_k \times C_k\right]_B \times R_B\right)\right)$$

With this measurement tool, I was able to analyze a number of different cases of nation state conflict in cyberspace to determine which side gained cyberspace superiority and how strong that superiority was.

Findings from the Case Studies

I analyzed nation state cyberspace conflict for which there was sufficient information available in unclassified sources. It was very important that I coded the inputs using a consistent and repeatable methodology and I have placed the details of the coding methodology in appendix A. The analysis for each of the case studies can be found in either chapter 5 or appendix B. I have place the results below in table 13.

Table 13 – Summary of Cyberspace Superiority Case Studies

Year	Case	Presumed Attacker	Objective	Defender	Outcome
2007	Estonia	Russia	Replace Statue, Intimidate Former USSR States	Estonia	$RCSI_{Russia} = (-0.15)$ $RCSI_{Estonia} = 0.15$
2008	Georgia	Russia	Seize South Ossetia and Abkhazia	Georgia	$RCSI_{Russia} = 0.61$ $RCSI_{Georgia} = (-0.61)$
2009	South Korean/ US DDoS	North Korea	Shut down US and South Korean Websites	South Korea/US	$RCSI_{North\ Korea} = (-0.46)$ $RCSI_{US/South\ Korea} = 0.46$
2010	Stuxnet	US/Israel	Disrupt Iranian Uranium Enrichment	Iran	$RCSI_{US/Israel} = 0.08$ $RCSI_{Iran} = (-0.08)$
2011	March 2011 South Korean DDoS	North Korea	Shut down US/South Korean Gov Websites	South Korea	$RCSI_{North\ Korea} = 0.03$ $RCSI_{South\ Korea} = (-0.03)$
2011	April 2011 South Korean Bank Attack	North Korea	Disrupt Nonghyup Bank/ Embarrass South Korea	South Korea	$RCSI_{North\ Korea} = 0.51$ $RCSI_{South\ Korea} = (-0.51)$
2012	Aramco	Iran	Interrupt Aramco Oil & Gas Production	Saudi Arabia/ Aramco	$RCSI_{Iran} = (-0.30)$ $RCSI_{Saudi\ Arabia} = 0.30$
2013	2013 South Korean Bank Attack	North Korea	Disrupt South Korean Banks and Media Companies	South Korea	$RCSI_{North\ Korea} = (-0.33)$ $RCSI_{South\ Korea} = 0.33$

Despite the predictions of some advocates, the cyberspace "bomber" does not always get through and the offense only seems to have a slight advantage. Out of eight case studies, the attacker had greater cyberspace superiority in four of them and the defender had greater cyberspace superiority in the other four. There was also a wide range in the superiority combatants achieved on both the offensive and defensive sides. There are no cases where a clearly weaker attacker succeeded, but I cannot conclude that either the offensive or defensive has superiority based on case study evidence. I can conclude that neither the offense nor defense has overwhelming superiority, as offenders and defenders both had varying levels of success. In addition, from the previous study of cyberspace characteristics, I expect that the offense will have a slight advantage, but that advantage will normally be very short lived.

The persistence of cyberspace superiority was less than two weeks in seven of the eight cases, leading to a conclusion that cyberspace superiority will not normally be persistent. The one case where the attacker managed significant persistence measured in years was the Stuxnet attack. The attackers managed long persistence in this case because the defenders did not know they were under attack and the designers of Stuxnet worked very hard to keep the weapon hidden.

I can draw two conclusions from this data on persistence. One is that the majority of cyberspace attacks only persist for approximately two weeks or less, and the second is that a weapon that can remain hidden is the only proven method of achieving long persistence of cyberspace superiority. Once defenders understand that they are under attack, they will react quickly and bring in the resources they need to stop the attack.

Another conclusion I can pull from the case studies involves universal cyberspace superiority.

Universal cyberspace superiority is not achievable, and combatants should not pour significant resources into pursuing it. In none of the cases did a combatant achieve any amount of universal cyberspace superiority. There is not even much evidence of a combatant achieving cyberspace superiority in multiple local areas simultaneously. Cyberspace is fragmented into countless local areas, based not just on geographic location, but multiple local areas can exist in the same physical location through various systems. In a single command center for example, there are normally numerous systems at different levels of classification that are separate local areas of cyberspace. In addition, universal superiority in cyberspace would need to be global. In the air domain, it is possible for a combatant to have universal superiority in a theater of operations such as the Persian Gulf. In cyberspace this geographic separation of theaters is not possible and a combatant may have servers and nodes spread over the entire globe. Thus to achieve universal cyberspace superiority a combatant would have to achieve global cyberspace superiority over all of cyberspace, which is not an attainable goal by any combatant. What a combatant can achieve is significant advantage for military operations through local cyberspace superiority.

Despite the relatively limited number of cases available, there are at least three cases that show cyberspace superiority providing significant advantage for military operations. In the Russia versus Georgia case, Russia accrued advantages to their conventional forces they would not have had without the cyberspace attacks. The disruption of the Georgian communication networks had a significant effect on the

Georgian ability to resist the invasion, and the other Russian attacks increased the pressure on Georgia to concede. The Russians achieved a high level of cyberspace superiority, but even a small one can bring some advantage as with Stuxnet.

The small level of cyberspace superiority attained by the U.S. and Israel with Stuxnet was able to provide them some significant advantages they could not have gotten from operations in the other domains. The level of cyberspace superiority achieved by the United States and Israel, small as it was, was sufficient to prevent a kinetic strike, as the attackers were able to slow the Iranian nuclear program without kinetic weapons. The strategic effect was to prevent kinetic operations that would likely have gone very badly, and to buy time for negotiations to find a solution. There is one other case where it is easy to see a combatant accruing a significant advantage for military operations.

The third case where a cyberspace combatant gained significant advantage for military operations through cyberspace superiority was the 2011 bank attack by North Korea. This attack resulted in significant advantage in military operations for the North Koreans as it gave them a very low risk way to attack their enemies that was not available in other domains. If the North Koreans had accomplished the same damage from a physical domain, they would not have been able to escape punishment by the international community. Since they used cyberspace, they were able to do significant damage, and still avoid serious consequences. Even with the limited cases available, there is good evidence that higher levels of cyberspace superiority correlate to advantage in military operations.

Limitations of the Study

There are several limitations to modeling and analysis in this study including that the model excludes third party actors. This can be especially problematic in cyberspace due to the difficulties of attribution where an actor may provoke conflict between two other nations. As a hypothetical example, if the United States power grid collapsed under attacks that appeared to originate in China, it could provoke a conflict between the two countries that might be very much in the interest of any number of other countries able and willing to make it appear as if the Chinese were behind the attack. The model as currently structured does not incorporate these types of complex but very important dynamics. Another complex arena that this study does not address is the nexus between war and politics.

Analysts of fourth generational war such as William Lind and Thomas Hammes discuss warfare when one of the participants is not a nation state. This study focused exclusively on interactions among nation states and while there will be some similarities, there will also be significant differences. Accordingly, one of the limitations of this study is that I did not examine these differences as they lay beyond the boundaries of the question I was researching.

A major limitation of this study that has been mentioned before but is worth highlighting is the paucity of the evidentiary base. Since there are so few relevant case studies to utilize, much of this study is conceptually based and needs to be refined and tested against new cyberspace conflicts as they occur. These future cases will provide refinement for the theories here as new evidence becomes available.

The measurement concept utilized in this study focused on the past and analyzing what occurred so that predictions could be made on how similar conflicts might unfold in the future. If the tool was to be utilized to predict outcomes, it would need to incorporate a probabilistic term to account for the level of confidence that a combatant would achieve a certain level of success against an objective. Adding in a probability to each objective or system functionality term in the equation could easily do this.

A final limitation of this study is that is focused on the operational level of warfare. I was examining the accomplishment of operational advantage through gaining cyberspace superiority, I did not delve into if that operational advantage would lead to strategic success. Many militaries have found to their sorrow that operational advantage does not automatically translate into strategic success but that was not the focus or within the scope of this project. While these are questions this project did not address, what it did address was if cyberspace superiority provided operational advantage.

Conclusions

If a nation achieves cyberspace superiority during a conflict, then it gains a significant advantage for military operations. Cyberspace superiority provides advantages at the tactical, operational, and strategic levels. The Russian and Georgian case study shows some of the advantages enjoyed by the Russians at the tactical level when their enemies could not communicate effectively. The 2011 North Korean case shows advantage generated at the operational level of war with the North Koreans gaining an operational advantage that they could not have gained using conventional military forces without isolating themselves further from the international community.

Finally, the Stuxnet case shows a combatant achieving a strategic advantage by using a cyberspace weapon enabled by cyberspace superiority.

While the number of cases of nation state warfare in cyberspace is small, theory and practice in the other domains also leads to the expectation that cyberspace superiority should provide significant operational advantage. Domain forces have always first attempted to achieve superiority their domain before they were able to utilize that superiority to have effects in other domains.[7] While armies have not often seen land warfare in these terms, both marine and air domain operators understand the need to establish superiority in their domain before they can provide support to the other domains. Cyberspace operators face the same situation, although superiority in their domain has different characteristics than the maritime and air domains as discussed previously. One area where these different characteristics stood out was in the interplay between the universal and local levels of superiority in the different domains.

One of the important insights that came out of this study of superiority in the different domains was the connection between universal and local domain superiority. The details change for each of the domains, but in general, local superiority is what matters when determining who can accomplish their objectives without prohibitive interference. Local superiority tends to be much more transitory than universal superiority, but local and universal superiority feedback into each other. The level of universal superiority determines the forces that are available in the conflict for local

[7] Thomas David McCarthy, "Traveling Domain Theory: A Comparative Approach for Cyberspace Theory Development" (PhD diss., Fletcher School of Law and Diplomacy, 2012), 188.

superiority and the losses incurred in the local engagement then feed back into the level of universal superiority. This finding leads directly into my first supporting question.

My first supporting question was whether domain superiority in general and cyberspace superiority in particular was a universal or local phenomenon. As I discussed earlier, the answer borne out by my research is yes, it is both a universal and local phenomenon but for cyberspace superiority, the local level is far more important. On the universal level are the assets that have theater-wide impact such as main armies, battle fleets, or strategic air defenses. On the local level are the smaller units and tools that only have reach to affect some smaller segment of the overall theater. The universal and local levels interact, and there is more importance to universal or local depending on the domain. In the cyberspace domain, the universal level is very hard to influence so both attackers and defenders will do the vast majority of their work on the local cyberspace superiority level. The answer to my second supporting question largely flowed from the answer to the first in that cyberspace superiority will normally be limited to the local level.

The second supporting question was how persistent domain superiority would be. The answer is that in the cyberspace domain, the persistence is very low. From a theoretical perspective, I have demonstrated why local cyberspace superiority tends to be so transitory. Universal superiority is more difficult to achieve in the cyberspace domain than in the land, maritime, or air domains and in each of the domains, it is the universal domain superiority that tends to be persistent. While local superiority is the one that will determine whether an attacker achieves a particular objective or not, the universal domain superiority is what produces the resources used in the local conflicts. Since universal

domain superiority is so difficult to achieve, most conflicts in cyberspace will be determined at the local level, which tends to produce transitory effects. I can provide further corroborating evidence for this theoretical model from the case studies. Out of eight case studies, seven of the conflicts lasted two weeks or less. Whatever level of cyberspace superiority that an attacker achieved either was lost by the termination of the conflict, or by the defense developing countermeasures that made the offensive weapons in use ineffective. Measuring the level of cyberspace superiority during a conflict was the next challenge.

My final supporting question was how a combatant could measure the level of cyberspace superiority. In the measurement section, I showed how analysts can use a weighted preference methodology to measure offensive success by summing the level of objective achievement along with the weight of those objectives, and how to measure defensive success by summing the level of functionality of key systems with along with their criticality. When I coded the inputs according to the methodology in appendix A and applied it to the case studies, the measurement system generated useful results. As this study progressed, several themes stood out that lead to implications for cyberspace warriors.

Implications

At the conclusion of this study, there are several implications that I can pull from the research findings for the practice of cyberspace operations.

Implication 1: Do not neglect cyberspace defenses

The cyberspace "bomber" did not, and does not always get through. In much of the commentary on cyberspace, there has been a great deal of discussion about how inherently offensive cyberspace is. The offensive in cyberspace does bring certain intrinsic advantages due to the characteristics of offensive cyberspace weapons. However, good defenses can make attacks much more difficult, and perhaps more importantly, reconstitute and rebuild systems quickly. The same rapid pace of action available to attackers also helps defenders, and while offensive cyberspace weapons are fast, they also rapidly lose their potency as defenders close vulnerabilities and update defensive systems to find and disable the new weapon. Offensive cyberspace warriors can deliver lightning fast blows with razor sharp swords, but by the end of the week, those swords tend to be foam rubber and useless, while the holes in the opponents armor have been patched and reinforced. Accordingly, cyberspace operators should not neglect the defensive side of the domain and place appropriate resources and emphasis on building and maintaining a good defense. This does not just apply to military systems but also to strategic industry and infrastructure such as critical defense related companies and the power grid.

Implication 2: Focus on local cyberspace superiority, but attack enemy universal resources whenever possible

Most cyberspace superiority will be local and temporary. The best method to achieve persistent cyberspace superiority is to attack enemy cyberspace warriors but they will be very hard to reach. There may also be some value in attacking communications hubs depending on the enemy's communications architecture. Targeting enemy cyberspace warriors will be very difficult, and temporary local cyberspace superiority

may be all that is required to achieve friendly objectives. Accordingly, most of the focus of a cyberspace combatant should be on gaining just enough local cyberspace superiority to achieve his objectives.

Implication 3: Attackers and defenders in cyberspace should assume a dynamic enemy who will often react in unexpected ways

This implication is a lesson from all of warfare that is not specific to cyberspace; however it bears repeating as analysts and planners forget it so often. Cyberspace is a high technology domain and there is always the temptation to technological determinism, where attackers and defenders inappropriately discount the enemy's potential to maneuver. This lesson is borne out by the case studies where each side continuously maneuvered, even if unsuccessfully. Despite their severe disadvantages, even the Georgians attempted several maneuvers from moving their servers out of Georgia, to placing fake attacking software on Russian websites that claimed to be attacking Georgia but was really attacking Russia. In each case study, there is clear evidence of dynamic maneuvering between the combatants.

Implication 4: Cyberspace operators should use a methodologically rigorous measurement system for training, planning, and exercises

Planners can easily use the measurement system developed here in training, planning, and exercises as a structured way to determine how simulated combatants are doing. Trainers could use this measurement system in exercises with trainees. Planners could incorporate the measurement system into wargaming to exercise potential courses of action. Referees could utilize a computer-aided system incorporating these measurement tools that could track each unit's progress. This measurement system could

provide an objective way to score the performance of different units and provide better feedback to commanders.

Future Research

There are several potentially profitable areas for further research. First of all, the data set for cyberspace conflict is extremely limited and the data sources are not very detailed. Future cyberspace conflicts between nation states are nearly inevitable and as they occur, the models and measurement methodology developed here can be further tested and refined. Especially problematic is that the only case of cyberspace conflict during a conventional campaign is the short Russian campaign in Georgia. Future armed conflicts between modern nations will involve cyberspace components, but there are currently no other cases to examine, which makes any conclusions about the importance of cyberspace superiority in a conventional conflict somewhat tentative.

Secondly, further case studies might provide an opportunity to examine in greater detail what factors lead to cyberspace superiority. There are several possible contenders including quality or quantity of people, successful intelligence, or physical resources. With the current data set, it is not possible to draw firm conclusions on the contribution to cyberspace superiority made by these various elements; future data should permit work in this area.

Finally, there is great need to study the connection between means, ways and ends in cyberspace. This study focused exclusively on means and ways, but connecting cyberspace means and ways with policy ends is an area in need of study. Unfortunately, cyberspace operators can sometimes become entranced with what they can do, and not

carefully examine what they should do. There are many complex interconnections between cyberspace ways and policy ends that would be well worth researching.

Final Conclusion

Cyberspace is a unique domain, but not so unique that the logic of war and strategy applicable in the other domains does not apply. To repurpose Clausewitz, "Its grammar, indeed, may be its own, but not its logic."[8] Cyberspace warriors need to guard against a tendency towards technological determinism and the dynamic interaction with the enemy will be impossible to predict with accuracy. Strategy's paradoxical nature explained by Luttwak, where you often get the opposite of what you are trying to get due to the enemy's responses, applies fully to cyberspace as well.[9] Both sides will be actively pursuing cyberspace superiority in an interactive manner, but they will each likely only be able to achieve local and transitory superiority.

Superiority in cyberspace is achievable and desirable, although it will be difficult to attain in more than a local and temporary form. Unlike the land, maritime, and air domains, offensive cyberspace forces do not engage in combat if they cross paths in cyberspace. Losses are normally only produced in local fights between offensive and defensive forces. The defensive forces also do not "destroy" offensive weapons; they render them impotent by patching vulnerabilities and updating detection systems. In some ways, the medical analogy suggested by Paul Rosenzweig is a better mental

[8] Carl von Clausewitz, *On War,* ed. and trans. by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 605.
[9] Edward N. Luttwak, *Strategy: The Logic of War and Peace* (Cambridge, MA: Belknap Press, 2003), 2.

template than traditional combat.[10] Good cyberspace defenses have more similarity to vaccines and medical care than infantrymen and artillery. Cyberspace defenses fight the current infection and restore the patient to good health, while inoculating him from any further infection. Also like medicine, if there are opportunities to drain swamps and decrease the total number of diseases in the world, cyberspace warriors should attempt to reduce the enemy's universal capability when possible.

Just because it will be difficult to achieve universal cyberspace superiority does not mean that combatants should not seek and attack universal cyberspace targets whenever possible, as degrading the enemy's universal cyberspace resources will make the local fights easier. The connection between the two goes both ways, and while a nation should not put too many resources into chasing difficult universal cyberspace superiority targets, there will be times when those targets are accessible. Generally, a kinetic strike in the physical domains is the easiest paths to lasting effects, but only if the targets are expensive and hard to replace. Simple servers and computers will normally not be productive targets. Even if attacks on infrastructure and cyberspace personnel are wildly successful, it does not guarantee a combatant's victory in the overall conflict.

Cyberspace superiority is neither necessary, nor sufficient, but it is important and will provide a significant advantage to a combatant who achieves it. The ability successfully to execute cyberspace operations is only part of a balanced national security portfolio for any nation. Offensive cyberspace operations can play two major roles, it can directly attack targets to produce effects, and it can provide support to other domain

[10] Rosenzweig, *Cyber Warfare*, Kindle Location 3727, chap. 16.

forces. At the current time and for the foreseeable future, the support cyberspace forces provide to the other domains is more important than the ability to produce direct effects. Nations should not neglect strategic information warfare, and there will be cases where it is the only or best option, but cyberspace operators need to remember the lessons of the early airpower theorists and not focus so much on producing strategic effects that they overpromise and under-deliver. In the United States, cyberspace operations have many of the same organizational and institutional issues that made the rise of airpower so difficult within the defense establishment. A balanced focus on what cyberspace can provide to the other domains with the ability to produce strategic effects will help ease the transition.

Cyberspace is here to stay from toilets to electrical grids. A modern nation should thoroughly study the past and build capable forces to contest and create superiority in the new domain of cyberspace.

APPENDIX A – CODING OF MEASUREMENT INPUTS

One of the greatest difficulties with measuring cyberspace is that an analyst cannot easily quantify the inputs. An analyst can construct an elegant and complex weighted preference model, but if he or she does not carefully code the inputs into the model, the output will not be useful for analysis or study.

The purpose of this appendix is to detail the definitions used in coding the various inputs that went into the measurement system developed in chapter 4. The intent is that different analysts could use these definitions to get similar inputs given similar data for a case study. Of course, there will be some variation, but I will provide examples to illustrate each of the levels for the input variables where appropriate, along with an explanation of how the weighing factors and system criticality variables can be determined. The first variable to examine is the level of success.

Level of Success (S)

The first critical input to the measurement model is level of success (S), which is the amount of success an attacker achieves against a particular cyberspace objective. To determine the value of this variable, a researcher needs to understand what objective an attacker is attempting to achieve from whatever data sources are available. Then the analyst can quantify that data as an input from 0.00 to 1.00 per the following table.

Table 14 – Level of Success (S) Coding

Description of Level of Success Coding	Level of Success (S)
Complete success, objective accomplished	1.00
Extremely successful against objective	0.90
Very successful against objective	0.80
Successful against objective	0.70
Mostly successful against objective	0.60
Achieved approximately half of objective	0.50
Somewhat successful against objective	0.40
Little success against objective	0.30
Minimally successful against objective	0.20
Almost no success against objective	0.10
Complete failure, no objectives achieved	0.00

A researcher can extrapolate between two levels of success to assign a 0.25 for example, but this extrapolation will rarely be required as the 10 levels available provide sufficient discrimination. Researchers should avoid making the inputs look more precise than they actually are as these values are normally going to represent quantification of incomplete and ambiguous data sets.

To assign S = 1.00, every part of an objective must have been reached. This category is one of the easier to assign, yet one of the more difficult actually to achieve for a protagonist. For example, if the objective was to take down a power grid, S=1.00

would imply that the power grid was completely non-functional and was not providing any power anywhere to any customer. If the objective were to disrupt cellular communications, then S = 1.00 would imply that there was no cell phone service operable anywhere in the targeted area.

To assign S = 0.90, an attacker must have been extremely successful against the desired objective. In this case, the attacker must have accomplished almost his entire objective with a negligible reduction in some minor area. For example, If the objective was to disrupt cellular communications, and one cellular tower was partially functional allowing a handful of calls in an unimportant remote area, that would be assigned S = 0.90.

To assign S = 0.80, the attacker was very successful against the desired objective. The difference between S = 0.80 and the previous ranking is that while the attacker still achieved what he intended to achieve, there are minor areas where success was not complete. As an example, if an attacker was attempting to disrupt the operations of a bank, but ten percent of the bank's ATM machines still worked, that would represent S = 0.80. The attacker has fully disrupted the bank the target will suffer large losses in revenue and public trust despite the ability of some of the bank's customers to access their accounts.

To assign S = 0.70, an attacker must have been successful against the desired objective. In this case, the attacker has achieved what he or she set out to achieve, although he or she may not have been successful in all areas. For example, if the attacker's objective was to disrupt a command and control system, and 25% of the system was still functional, S = 0.70 would be appropriate if the overall system could not

function effectively. As another example, if an attacker was attempting to disrupt a logistics system, and elements of the system stayed functional but the system could not effectively move resources across the theater that would represent S = 0.70.

To assign S = 0.60, an attacker must have been mostly successful against the desired objective. For example, if an attacker was trying to take down a power grid to disrupt an area, and 30% of the grid stayed functional, then that would represent S = 0.60. In this case, the attacker has not completely met his system objective. Some relatively unimportant part of the enemy system is operational despite the attack affecting the majority of the system as intended.

To assign an S = 0.50, the attacker must have achieved approximately half of the desired objective. In some cases, this circumstance will be easy to measure. For example, if an electrical grid is attacked and is still providing power to 50% of its customers, that would represent S = 0.50. Other cases will depend more on a qualitative analysis suggesting that an attacker accomplished only half of a desired objective. An example of this situation might be a North Korean objective to embarrass the South Korean government. If public opinion and news coverage seems to be split, assigning S = 0.50 would be appropriate.

To assign S = 0.40, the attacker must have only achieved partial success against his objective. The attacker should have accomplished less than half of what he wanted, but he still accomplished something of significance. In an attack against a bank for example, the attacker might have been able to force some branches in a limited number of cities to close, but the majority of the bank's branches were able to remain open and

serve customers. The attacker did real damage to the bank, but the bank was still able to function at a reduced capacity.

To assign S = 0.30, the attacker had little success against his objective. For example, in an attack against a power grid, the attacker was able to shut down ten percent of the power grid's customers. The attack still accomplished something of value to the attacker, but the effects achieved were disappointing.

To assign S = 0.20, the attacker had minimal success against his objective. For example, an attack against a communications system might have slowed the system somewhat, but the enemy is still able to utilize the system. A real world example is the North Korean attempt to take down a number of South Korean Government websites in 2011. Some web sites were affected, but only a few, and only for a short period of time.

To assign S = 0.10, the attacker had almost no success against his desired objective. An example of this circumstance might be if an attacker was attempting to take down a power grid, and succeeded in knocking out a few substations, but defenders were able to reroute with no loss of power to customers. The attacker successfully disrupted some elements of the system, but the overall system continued to function effectively. As another example, a rating of S = 0.10 would be appropriate if an attacker attempted to disrupt a communications system but only succeeded in negligibly slowing traffic. There was some effect, but it did little to advance the attackers agenda.

To assign S = 0.00, the attacker had no success at all against the desired objective. Some elements of the attack might have been technically successful, but the attacker achieved none of his goals. The Russian attacks against Estonia in 2007 provide an example of this situation. While some of the cyberspace attacks produced various

effects, the statue that the Russian government wanted returned to its former site remained in place in its new location. The next factor that we need to consider on the offensive side is the weighing factor that accounts for the importance of each level of success in the model.

Weighting Factor (W)

I use the weighting factor to account for the different levels of importance that an attacker has for his various objectives. The mathematical sum of all the weighting factors must always equal 1.00, which represents 100%. If an attacker has only one objective, than W = 1.00. If there is more than one objective, than a researcher should determine the weighting factors by considering how important each objective is to the attacker in relation to each other. For example, if an attacker had two objectives and objective 1 was three times more important than objective 2, then $W_1 = 0.75$ and $W_2 = 0.25$. If there are multiple objectives, then an analyst compares the relative importance of all objectives against the other objectives. The weighting factor says nothing about the absolute importance of the objective to the attacker, only the relative importance in relation to the other cyberspace objectives the attacker pursued as part of the same conflict.

Level of Functionality (L)

On the defensive side, analysts should think of the level of functionality (L) in a similar way as the level of success (S) on the offensive side of the measurement construct. Level of functionality captures how effectively defenders are protecting their systems. L is a measurement of the health of the friendly system, not how strong or weak the enemy attack was. A strong attack that a defender was successful against and a weak

attack that was an attacker was less successful against would receive the same rating if the system effectiveness was the same in both cases. The level of functionality ranges from 0.00 to 1.00 in accordance with table 15.

Table 15 – Level of Functionality (L) Coding

Description of Level of Functionality Coding	Level of Functionality (L)
System is fully functional with no degradation	1.00
System is functional with negligible degradation	0.90
System is functional with minimal degradation	0.80
System is functional with little degradation	0.70
System is functional with some degradation	0.60
System has half of its normal functionality	0.50
System functional with significant disruption	0.40
System is functional with major disruption	0.30
System is minimally functional	0.20
System is barely functional	0.10
System is completely inoperative with no functionality	0.00

Just like with level of success on the offensive side, researchers can extrapolate between the levels although this extrapolation will not often be required or useful given the typical issues with the data set. If the attacker had no measurable effect on the defended system, then L = 1.00 is the appropriate rating. Assigning this value can be appropriate even if the attacker had some success against other areas, but not the system under consideration. As a real world example, when the Iranians attempted to shut down oil and gas production at Aramco, they disrupted a large number of support computers,

but oil and gas production was not effected so the oil and gas production system still maintained L = 1.00.

If the attacker only produced negligible disruption to the defended system, then L = 0.90 is appropriate. The attacker may have had limited success against peripheral or unimportant parts of the defended system, but it was barely noticeable. An example of this situation is the North Korean attacks of 2009 against U.S. government web sites. The attack slightly affected a few poorly defended web sites such as ones at the Department of Transportation, but the attack did not affect more important sites such as those at the White House and Department of Defense.

To assign L = 0.80, the defended system should be functional with only minimal degradation. You can see a real world example of this circumstance in the North Korean 2013 attacks against several South Korean banks. While the banks suffered some systems degradation, they were able to continue to function with little disruption for their customers.

To assign L = 0.70, the defended system should be functional with little degradation. In the North Korean 2013 bank attacks, had South Korean banks been forced to close a few branches for a short period of time affecting a small percentage of their customers, then L = 0.70 would be appropriate. At L = 0.70 there has been disruption, but it is not yet of much significance.

To assign L = 0.60, the defended system should have experienced some disruption, but it is still more than 50% functional. For example, if a power grid were attacked and 75% of the power grid's customers still had power, that would represent

L = 0.60. There was real disruption, but the system overall continued to function well above 50% effectiveness.

To assign L = 0.50, the defended system should be at approximately 50% effectiveness. This rating applies to easily quantified systems such as power grids and telecommunications, as well as systems that are more difficult to quantify. A real world example of a system at 50% is the South Korean broadcasters in 2013 that did not go off the air, but lost many of their support systems, which significantly affected their ability to produce material and cover news events.

To assign L = 0.40, the defended system should be experiencing significant disruption and be operating at less than 50% efficacy. For example, a command and control system that had lost the ability to communicate with more than 50% of its nodes, but still could effectively control some areas would be at L = 0.40.

To assign L = 0.30, the defended system should be experiencing major disruption. To return to the power grid example, a power grid that is only providing power to 25% of its customers would be at L = 0.30. The system still has some capability, but it is well less than 50% functional.

To assign L = 0.20, the defended system should be minimally functional. As a real world example, Georgia in 2008 could relay government communications, but only with great difficulty and through abnormal channels. The regular communications links between the Georgian government and its military forces were under significant attack and only functioning intermittently.

To assign L = 0.10, the defended system should be almost completely non-functional. Some elements of the system may still be operational, but as a complete system, it has barely any useful functionality.

To assign L = 0.00, the defended system has lost all ability to perform any part of its designed functionality. The support system network in the Aramco attack is an example of this situation where the attacker successfully destroyed the entire network, which Aramco had to rebuild completely from the ground up. In the power grid example, to assign an L = 0.00, the power grid should not be providing any power to any portion of its customers. The level of effectiveness is one of the important defensive inputs the second is system criticality.

System Criticality (C)

System criticality (C) fulfills the same function on the defensive side that the weighting factor (W) does on the offensive side and operates in a similar way. System criticality brings into the model the importance of the various defended systems to the defender and it must add up to 1.00, or 100%, for a particular conflict under study. If there are multiple systems under attack, then their relative importance to the defender sets the values. If a defender has three systems under attack and one of them is twice as important as the other two then $C_1 = 0.50$, $C_2 = 0.25$, and $C_3 = 0.25$. The final measurement system input we should consider is a nation's reliance on cyberspace.

Reliance on Cyberspace (R)

Reliance on cyberspace (R) brings a relative measurement of the importance of cyberspace into each member of the dyad under consideration. It is a relative

measurement to the two nations under consideration so a nation's R will change depending on who is the other nation an analyst is comparing. For example, if nation A with a moderate level of reliance on cyberspace was paired with nation B, which was extremely dependent upon cyberspace the values might be $R_A = 0.30$ and $R_B = 0.70$. However, if nation A was paired in a different conflict with nation C that had minimal reliance upon cyberspace then the values could be $R_A = 0.80$ and $R_C = 0.20$. Both R values in a dyad must always add up to 1.00 or 100%. The reason why R is relative is that the output of the measurement system is also relative. Cyberspace superiority in a conflict is a relative measurement between two combatants, and their absolute reliance on cyberspace is not as important as their relative reliance on cyberspace.

APPENDIX B – ADDITIONAL CASE STUDY ANALYSIS

This appendix will provide a more detailed look at the analysis and inputs behind the case studies with the exception of the cases covered in detail in chapter 5.

Russia versus Estonia 2007

There are several significant features of the Estonian cyberspace attacks of 2007 for the study of cyberspace superiority. The Estonian attacks were the first case of overt nation-state vs. nation-state cyberspace conflict. The conflict pitted a large and powerful country against a small, but technologically competent one. It was also the first use of "patriotic hackers" by a state to provide some level of plausible deniability to their actions. Finally, the defenses held and Estonia was able to maintain cyberspace superiority, while the Russians did not accomplish their most important objectives. To analyze these attacks, we first look at the offensive inputs.

Offensive Level of Success (S) and Weighting Factor (W) in Russia vs. Estonia 2007

The first step of calculating the offensive cyberspace superiority inputs into the measurement model is to determine the identity of the attacker. While there was no concrete attribution to the Russian government, there is enough circumstantial evidence to find it likely that the Russian government encouraged the attacks even if they did not direct them. The Estonian Prime Minister Andrus Ansip directly accused the attacks of originating "from the servers of Russian state authorities," although the Estonian government later admitted they did not have conclusive proof.[1] Several years after the attacks, a Russian official from the pro-Kremlin Unified Russia party, Sergei Markov, admitted that one of his assistants was responsible for the attacks but claimed that the

[1] Jared Moya, "Massive DDoS attacks target Estonia; Russia accused." Zeropaid, 14 May 2007, http://www.zeropaid.com/news/8759/massive_ddos_attacks_target_estonia_russia_accused/.

attack was actually "cyber defense."[2] A leader of a Pro-Kremlin Russian youth organization "Nashi," Konstantin Goloskokov, who may have been the "assistant" also verified Nashi's involvement in an interview with the Financial Times.[3] While this evidence does not prove collusion, when you consider that Nashi was also heavily involved in the Georgian cyberspace attacks where there was clear evidence of collusion, it suggests official sponsorship and support. Accordingly, I coded this case as a cyberspace attack by Russia on Estonia. Because Russia did not claim responsibility, I had to infer their objectives.

The next step in defining the offensive inputs is to determine the attacker's objectives and the main Russian objective was to coerce Estonian into replacing a World War II Soviet memorial. The attacks occurred after the Estonian government moved the memorial and ethnic Russians in Estonia rioted. Russia attempted to force Estonia to replace the statue and apologize through a range of measures from mysterious "railroad maintenance" cutting off Estonia's commerce, slowing oil shipments, political pressure and the cyberspace attacks.[4] Of course, the statue was important to the Russians principally as a symbol of their continuing influence, not just as a physical object.

The second Russian objective was to use the conflict with Estonia to demonstrate to the other former Soviet republics that they should give in to Russian demands. This objective was always in the background of the conflict given that Estonia had recently

---

[2] Dan Goodin, "Kremlin-backed youths launched Estonian cyberwar, says Russian official." *The Register*, 11 March 2009, http://www.theregister.co.uk/2009/03/11/russian_admits_estonian_ddos/.
[3] Noah Shachtman, "Kremlin Kids: We Launched the Estonian Cyber War." *Wired*, 11 March 2009. http://www.wired.com/dangerroom/2009/03/pro-kremlin-gro/.
[4] Meera Louis and Ott Ummelas. "Estonian Premier Says Internet Attacks Not Acceptable (Update2)" *Bloomberg*, 24 May 2007.
http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a9C66FjyCFBk&refer=europe.

joined the EU and NATO over Russian objections. The Russians saw this situation as an opportunity to flex their muscles and demonstrate that there would be a price to pay for going against their wishes. Unfortunately for the Russians, their attempted intimidation was not very successful.

Russia made little progress towards its objectives. The statue stayed where it was and the Estonian government refused to back down so I set $S_1 = 0.00$. The Russians were also only minimally successful in intimidating neighboring states. The Baltic States continued to move further out of the Russian orbit and Georgia continued refuse to bow to Russian pressure, which led to the Georgian conflict a year later. Russia was minimally successful in at least showing that there would be a price for going against her interests and so I set $S_2 = 0.20$.

It was unclear exactly how to weight these objectives. On the one hand, from a geopolitical perspective, the location of the statue was not very important compared to the respect shown to Russian interests by neighboring countries. On the other hand, the statue became a powerful symbol that received an immense amount of attention in Russian media. I therefore assigned equal weight to both objectives and $W_1 = W_2 = 0.50$. The Russian offensive inputs into the cyberspace superiority measurement model are in table 16.

Table 16 – Russian Objectives in Estonian Attack

	Objective	Level of Success (S)	Weighting Factor (W)
1	Get the statue replaced	0.00	0.50
2	Intimidate other former Soviet states	0.20	0.50

These inputs yield $OCSI_{Russia} = 0.10$, which represents the lowest level of offensive cyberspace superiority of the eight case studies. As Estonia did not attack any Russian targets, $OCSI_{Estonia} = 0.00$.

Defensive Level of Functionality (L) and Criticality (C) in Russia vs. Estonia 2007

The second step in determining cyberspace superiority is to look at the defended systems and their functionality. While there were a number of different systems attacked across Estonia, the two that were most important were government and banking web sites.

The attacks initially affected the Estonian systems significantly; however, the defenders were able rapidly to reconstitute and so mitigated much of the damage. The attacks were simple Distributed Denial of Service (DDoS) with some web site vandalism and the attackers did not target critical information such as banking transactions. However, over the period of time that the attacks continued, the disruptions were initially very severe until Estonian defenses became more effective. Both systems appear to have had similar levels of functionality over time. In accordance with the coding matrix in appendix A, both systems were functional with major disruption so $L_1 = L_2 = 0.30$.

The banking system was more important in the daily life of Estonians than being able to access government web sites. As a result, I weighted the banking system four

times heavier than government web sites, which gives $L_1 = 0.80$ and $L_2 = 0.20$. The defensive inputs are in table 17.

Table 17 – Estonian Systems under Attack in 2007

	System	Level of Functionality (L)	System Criticality (C)
1	Banking System	0.30	0.80
2	Government Internet	0.30	0.20

With these inputs, $DCSI_{Estonia} = 0.30$ and as there were no Estonian attacks to defend against, $DCSI_{Russia} = 0.00$.

Relative Cyberspace Superiority Index in Russia vs. Estonia

The final major input into the model is how important cyberspace was to both nations. In 2007 Estonia was one of the most highly wired and connected countries in the world earning it the nickname "e-stonia." If Russia had experienced the same level of Internet attacks, it would have been less disruptive for Russian citizens because their dependence on cyberspace was much less. As a result, I set Estonia's reliance on cyberspace three times higher than Russia's reliance and assigned $R_{Russia} = 0.25$ and $R_{Estonia} = 0.75$.

All of these inputs combined gives:

$OCSI_{Russia} = 0.10$
$DCSI_{Russia} = 0.00$
$R_{Russia} = 0.25$
$OCSI_{Estonia} = 0.00$
$DCSI_{Estonia} = 0.30$
$R_{Estonia} = 0.75$

$CSI_{Russia} = 0.08$ and $CSI_{Estonia} = 0.23$, which yields:

$RCSI_{Russia} = -0.15$
$RCSI_{Estonia} = 0.15$

In this case, the aggressive Estonian defensive response and refusal to be intimidated resulted in a Russia not gaining enough cyberspace superiority to accomplish its objectives. The attacks were not a complete failure however, Russia clearly showed its neighboring nations that there would be a price for going against Russian interests, which is a lesson that Georgia would have done well to heed.

North Korea versus United States and South Korea in 2009

This was the first in a series of North Korean cyberspace attacks that had varying levels of success. In this case, North Korea did not establish cyberspace superiority and so did not gain any significant operational advantage as a result of these attacks.

Level of Success (S) and Weighting Factor (W) in 2009 North Korean Attacks

The first step in coding the offensive inputs into the cyberspace superiority measurement system is to determine who the attacker was. Attribution in this case is not definite, as North Korea has not admitted that it was behind the attack and the United States has not officially accused North Korea. However, South Korea's spy agency claimed that North Korea was behind the attacks and also claimed to have found the actual orders to the research agency affiliated with the North's Ministry of Peoples Armed Forces. Allegedly, the orders said the institute was to, "destroy the South Korean puppet communications networks in an instant."[5] These attacks also occurred in a time

[5] Associated Press, "North Korean army suspected in cyber attacks: Hackers told to 'destroy' South Korean communications, report says," *NBC News*, 11 July 2009. http://www.nbcnews.com/id/31866018/ns/world_news-asiapacific/.

of heightened tensions between North and South Korea and a few months after a Korean newspaper claimed that North Korea created a new cyberspace warfare unit.[6] There are even allegations that the current leader of North Korea, Kim Jong Un, was the commander of the unit that carried out the attacks.[7] Given the diplomatic realities in North East Asia, it is unsurprising that the United States is unwilling to identify publically North Korea as the attacker, but there is enough evidence to proceed with the case and identify the North Korean objectives.

As North Korea did not take responsibility for the attack, I have to infer their objectives from the target set. All of the attacks were Distributed Denial of Service (DDoS) attacks which attack access to Internet based web sites or services, but do not access information on the targeted systems.[8] The targets included government sites in both the United States and South Korea as well as the party web site of the conservative party in South Korea, and finally what can best be characterized as economic targets in South Korea and the US such as South Korean banks and the NASDAQ stock exchange.[9] The objective of the attacker appeared to be to damage US and South Korean governmental and economic web sites. Inferring what North Korea intended to gain from the attacks if they were successful is more challenging. Possibilities range from simply

[6] Korea Times. "N. Korea Operates Cyber War Unit." The Korea Times. 5 May 2009. http://www.koreatimes.co.kr/www/news/nation/2010/04/113_44358.html.
[7] Colin Clark, "US Blew NK Cyber Attacks." *DoD Buzz*, 13 July 2009. http://www.dodbuzz.com/2009/07/13/7833/.
[8] Korea Times, "Dreadful Cyber War." The Korea Times, 10 July 2009. http://www.koreatimes.co.kr/www/news/opinon/2009/07/137_48261.html.
[9] Lolita Baldor, "White House among targets of cyber attack: Other targets included NSA, Homeland Security and State Department," *NBC News*, 8 July 2009, http://www.nbcnews.com/id/31800532/ns/technology_and_science-security/.

trying to damage adversaries, to continuing the normal cycle of escalation, to establishing Kim Jong Un as a military leader who could damage North Korea's enemies.

The attacks on US government websites were only marginally successful. Major targets such as the Pentagon and White House successfully defended themselves with no loss of capability. Some, less well-defended federal agencies such as the Department of Transportation and the FTC experienced some difficulty, but the overall effect on the US government was barely noticeable.[10] In accordance with the coding matrix in appendix A, I therefore assigned $S_1 = 0.10$.

The attacks on the South Korean government websites were more successful with the official Presidential website and the defense ministry paralyzed during the initial attacks.[11] Some of the South Korean websites under attack were able to continue functioning so I set the overall $S_2 = 0.50$.

US economic sites experienced little disruption while some South Korean banking sites and an online auction system experienced difficulty.[12] As the North Koreans achieved almost no success against the US economic sites I set $S_3 = 0.10$. The attackers has slightly more success against the South Korean economic sites and achieved minimal success against this objective so I set $S_4 = 0.20$.

The relative weights were set to emphasize the government sites versus the economic ones as that were where the initial attacks focused. The attacks shifted to economic sites in the second wave after the attackers appeared not to get the results for

[10] Lolita Baldor, "White House among targets of cyber attack."
[11] Associated Press, "N. Korea Suspected of Global Cyber Attack," *NBC News*, 8 July 2009. http://www.cbsnews.com/stories/2009/07/08/tech/main5143457.shtml.
[12] Jane Han, "Cyber Attack Hits Korea for Third Day," *Korea Times*, 9 July 2009. http://www.koreatimes.co.kr/www/news/biz/2009/09/123_48203.html.

which they had been hoping.[13] I started by giving South Korea and the United States half of the weighting, and then I weighed each nation's government sites at four times the weight of the economic sites. I give the resulting weights in the objective table 18.

Table 18 – North Korean Offensive Objectives in 2009

	Objective	Level of Success (S)	Weighting Factor (W)
1	Shut Down US Government websites	0.10	0.40
2	Shut Down South Korean Government websites	0.50	0.40
3	Shut Down US Economic websites	0.10	0.10
4	Shut Down South Korean Economic websites	0.20	0.10

These inputs yield an $OCSI_{North\ Korea} = 0.27$, which is the third lowest of the eight cases. South Korea and the United States had no offensive objectives so $OCSI_{US/South\ Korea} = 0.00$.

Level of Functionality (L) and Criticality (C) in 2009 North Korean Attacks

The next step is to determine the defensive inputs for the cyberspace superiority measurement system. On the defensive side, both the United States and South Korea were very active. Computer security firms bolstered the systems under attack, attacking IP addresses were cut off, and South Korea went so far as have the Korean Communications Commission (KCC) order service providers to deny access to 30,000

[13] Lolita Baldor, "US officials eye North Korea in cyber attack," *Tulsa World*, 8 July 2009. http://www.tulsaworld.com/article.aspx/US_officials_eye_North_Korea_in_cyber_attack/20090708_13_0_seouls64065.

South Korean computers that were part of the attacking botnet.[14] These defensive measures were largely successful.

The attacks against U.S. government websites were largely ineffectual, and the only sites affected at all were not critical ones. Therefore in accordance with the coding matrix in appendix A, I set $L_1 = 0.90$.

The attacks against South Korean government websites were more effective. However, the attacks had relatively short duration due to effective countermeasures by the defenders and the attacks only significantly affected some government sites so I assigned $L_2 = 0.50$.

U.S. economic websites continued at full functionality during the period of the attacks. Therefore, deciding on coding is relatively simple and $L_3 = 1.00$.

A few, relatively unimportant South Korean economic websites experienced some minor issues. However, the overall system experienced negligible degradation and $L_4 = 0.90$.

To weight the system criticality of the various systems, I mirrored the same technique I used in the offensive inputs of giving half the weight to each nation, and then weighting the government systems as four times the weight of the economic systems. The results are in table 19.

[14] Jane Han, "Cyber Attack Hits Korea for Third Day."

Table 19 – Critical US and South Korean Systems in 2009

	System	Level of Functionality (L)	System Criticality (C)
1	US Government websites	0.90	0.40
2	South Korean Government websites	0.50	0.40
3	US Economic websites	1.00	0.10
4	South Korean Economic websites	0.90	0.10

With these inputs, $DCSI_{US/South\ Korea} = 0.75$, which represents the third highest DCSI of the eight cases. As South Korea and the United States were not attacking North Korean systems, $DCSI_{North\ Korea} = 0.00$.

Relative Cyberspace Superiority Index in 2009 North Korean Attacks

North Korea does not rely nearly as heavily on cyberspace as the US and South Korea. There is minimal cyberspace connectivity in North Korea, and in 2009 it was only for government use. Accordingly I set $R_{North\ Korea} = 0.05$ and $R_{US/South\ Korea} = 0.95$. All of these inputs give:

$OCSI_{North\ Korea} = 0.27$
$DCSI_{North\ Korea} = 0.0$
$R_{North\ Korea} = 0.05$
$OCSI_{US/South\ Korea} = 0.0$
$DCSI_{US/South\ Korea} = 0.75$
$R_{US/South\ Korea} = 0.95$

$CSI_{North\ Korea} = 0.26$ and $CSI_{US/South\ Korea} = 0.71$, which yields:

$RCSI_{North\ Korea} = -0.46$
$RCSI_{US/South\ Korea} = 0.46$

This finding represents significant cyberspace superiority for the United States and South Korea. Both countries responded quickly to the attacks and took aggressive measures to cut off attacking systems. While there were stories in the press, there was little discussion of the attacks in the general media even shortly after the event and so North Korea failed to accomplish much other than to show that they were building capability in cyberspace. This attack was their first attempt and future North Korean efforts would have better success.

North Korea versus South Korea March 2011 Distributed Denial of Service

This case was another Distributed Denial of Service (DDoS) attack by North Korea, but it had several differences from the 2009 attacks. This attack was far more sophisticated while appearing on the surface to be another simple DDoS attack. The North Koreans were able to achieve a much higher level of cyberspace superiority than they did in their 2009 attack.

Level of Success (S) and Weighting Factor (W) in North Korean 2011 DDoS Attacks

The first step in calculating the level of cyberspace superiority was to determine who the attacker was so that I could determine their objectives. North Korea did not admit to this attack, but there are several reasons to suspect their involvement. One is that there were a number of similarities in the code and method of the attack that made it appear as if the same group that created the 2009 attack on South Korea and the United States was also behind the 2011 attack.[15]

[15] Infosecurity, "North Korea likely source of DDoS attacks against South Korean sites, says McAfee," *Infosecurity*, 7 July 2011. http://www.infosecurity-us.com/view/19258/north-korea-likely-source-of-ddos-attacks-against-south-korean-sites-says-mcafee/.

The target set is also highly suspicious as it included sites affiliated with the South Korean government, military and civilian critical infrastructure as well as U.S. Forces Korea and Kunsan AB.[16] There was not only overlap in the types of targets, 14 of the 40 specific targets attacked were also attacked in the 2009 attack linked to North Korea.[17] Finally, McAfee researchers have linked the 2009, 2011 and 2013 attacks through a piece of cyberspace espionage malware referred to as Operation Troy.[18] Since the same reconnaissance software links all the attacks, it is sensible to assume that the attacks came from the same source. Since there is reasonably good evidence in each of the attacks, the cumulative weight of the evidence that North Korea was behind all of them is substantial.

All of this evidence makes is very likely that North Korea was behind the attacks and I will attribute all three to them. I have to infer the North Korean objectives, as they did not announce their motives. There are several clues in the characteristics of the attacks, these were not normal DDoS attacks such as were launched in 2009.

The attacks were an odd combination of technical sophistication and brute force. The attackers deliberately destroyed and wiped their botnets at the end of the 10-day attack window, which is very unusual for any sort of hacktivist or criminal organization. Those organizations protect their botnets to keep them for future use. The North Koreans instead went to great lengths to encrypt their botnets at multiple levels and then wipe them to make it more difficult for researchers to track. However, the weapon itself was

[16] Kevin Kwang, "S. Korea, US attacks possibly launched by N. Korea," *ZDNet*, 6 July 2011. http://www.zdnet.com/s-korea-us-attacks-possibly-launched-by-n-korea-2062301087/.
[17] Kwang, "S. Korea, US attacks possibly launched by N. Korea."
[18] Ryan Sherstobitoff and Itai Liba, "Dissecting Operation Troy: Cyberespionage in South Korea," White Paper developed by McAfee Labs, 2013, 8.

an unsophisticated DDoS. McAfee Security sees this combination as evidence that the attacker's intent was to test the defender's response capabilities.[19]

The first objective appears to have been to test South Korean response and mitigation capabilities. The North Koreans were completely successful in this objective and were able to monitor the South Korean response. I therefore set $S_1 = 1.00$.

As the targets of the attacks were websites located in South Korea, shutting down those websites appears to have been an objective as well. That portion of the attack was only minimally effective and most of the targeted web sites were able to continue operating so I set $S_2 = 0.20$.

Given the continuing animosity between North and South Korea, North Korea is always looking for any way to embarrass or damage South Korea, which makes that a likely final objective. Unlike the 2009 attack, every site attacked was physically located in South Korea. There was not much press attention paid to these attacks and the South Korean response came across as competent and effective so this portion of the attack was also minimally successful and I set $S_3 = 0.20$.

I find the McAfee argument that this attack was primarily about reconnaissance compelling and so I placed the preponderance of the weight on that objective. I put four times the weight on the reconnaissance objective as the other two objectives combined, which gives $W_1 = 0.80$. I placed equal weight on the remaining two objectives, which gives $W_2 = W_3 = 0.10$. The offensive inputs for cyberspace superiority are in table 20.

[19] McAfee. "Ten Days of Rain: Expert analysis of distributed denial-of-service attacks targeting South Korea." White Paper developed by McAfee Security, 2011, 12.

Table 20 – North Korean Offensive Objectives in 2011 DDoS Attack

	Objective	Level of Success (S)	Weighting Factor (W)
1	Determine South Korean response and recovery capabilities	1.00	0.80
2	Shut Down South Korean websites	0.20	0.10
3	Embarrass South Korean government	0.20	0.10

These inputs yield an $OCSI_{North\ Korea} = 0.84$. As South Korea and U.S. Forces Korea had no offensive objectives, $OCSI_{South\ Korean} = 0.00$.

Level of Functionality (L) and Criticality (C) in North Korean 2011 DDoS Attacks

The second step in determining who had how much cyberspace superiority is to develop the defensive inputs. On the defensive side, South Korea immediately launched mitigation measures and was able to utilize previously installed digital "bunkers" that were IP addresses set aside for organizations that come under DDoS attack.[20] The North Koreans attempted to make it difficult to respond to the attacks as, "several steps were taken to ensure that the mission was executed without interruption, within the predefined attack window—and following, ensuring that all vehicles of attack would be destroyed, thus limiting forensic analysis."[21] However, within a few days, McAfee and others were able to "detect, reverse engineer, and mitigate the attacks."[22]

The disruptions for both South Korea and the U.S. military were short lived and both systems maintained a high level of functionality. The South Korean sites were slightly more effected by the attacks so I coded them as functional with minimal

[20] Kwang, "S. Korea, US attacks possibly launched by N. Korea."
[21] McAfee. "Ten Days of Rain," 3.
[22] McAfee. "Ten Days of Rain," 3.

degradation and set $L_1 = 0.80$. The U.S. military sites only experienced negligible degradation and so $L_2 = 0.90$.

The North Koreans attacked a far greater number of South Korean sites compared to a relative handful of U.S. military sites so I weighted the South Korean sites much more heavily. I placed 90% of the weight on the South Korean sites and only 10% on the U.S. military sites in South Korea. Accordingly, I set $C_1 = 0.90$ and $C_2 = 0.10$. The defended systems are in table 21.

Table 21 – Critical US and South Korean Systems in 2011 DDoS Attack

	System	Level of Functionality (L)	System Criticality (C)
1	South Korean government and military websites	0.80	0.90
2	U.S. military websites	0.90	0.10

With these inputs $DCSI_{South\ Korea} = 0.81$, which is the most successful level of defense achieved among the eight case studies. North Korea did not come under attack and so $DCSI_{North\ Korea} = 0.00$.

Relative Cyberspace Superiority Index in North Korean 2011 DDoS Attacks

North Korea does not rely nearly as heavily on cyberspace as the US and South Korea so $R_{North\ Korea} = 0.05$ and $R_{South\ Korea} = 0.95$. All of these inputs give:

$OCSI_{North\ Korea} = 0.84$
$DCSI_{North\ Korea} = 0.00$
$R_{North\ Korea} = 0.05$
$OCSI_{South\ Korea} = 0.00$
$DCSI_{South\ Korea} = 0.77$
$R_{South\ Korea} = 0.95$

$CSI_{North\ Korea} = 0.80$ and $CSI_{South\ Korea} = .77$, which yields:

$RCSI_{North\ Korea} = 0.03$
$RCSI_{South\ Korea} = -0.03$

While North Korea only established a very low level of cyberspace superiority bordering on neutrality, this case represented a significant step forward for North Korea in capability from the 2009 attacks. The mechanism used was more sophisticated and if their primary goal was to obtain data on South Korean defense and reconstitution methods, they succeeded in that goal despite the low level of damage done.

This case is also interesting because both the offender and defender were relatively successful as they were aiming at different things. The North Koreans were trying to learn about South Korean defenses, and the South Koreans were trying to keep their systems up and running. Both largely succeeded, which resulted in near neutrality in the overall cyberspace superiority. These attacks also set up the 2011 bank attacks, which were much more successful for North Korea.

North Korea versus South Korea April 2011 Bank Attack

Less than a month after the March DDoS attack, South Korea was under a major cyberspace attack again, and this time the North Koreans established a much higher level of cyberspace superiority.

Level of Success (S) and Weighting Factor (W) in North Korean 2011 Bank Attack

The first step to calculating cyberspace superiority is to establish who the attacker was on the offensive side to determine their objectives. Despite the accusations of South Korean prosecutors, North Korea flatly denied that it had anything to do with the attack, but there are again a number of reasons to doubt that claim. One is the linkage between

the previous attacks; one of the IP addresses used by the attackers to break into Nonghyup's system was the same as one used in the March 2011 attack.[23] The software used in the attack was also similar to that used in the July 2009 attack on South Korean and U.S. websites, which I attributed to North Korea previously.[24] Finally, given that North and South Korea are still technically at war and North Korea has shown a long and enduring propensity to attack South Korea whenever possible, it is reasonable to assume that North Korea is behind this attack as well. North Korea's denials are also interesting because they state it is a false accusation, just like the accusation that they sunk the *Cheonan*, a South Korean ship that exploded in waters close to North Korea.[25] Given that the physical evidence convinced the international community, with the exception of North Korea's close allies, that North Korea was behind sinking the *Cheonan*, this denial also rings false. Accordingly, I will attribute this attack to the North Koreans.

Once again, I will infer the North Korean objectives from the attack itself. The attack was specific to Nonghyup bank versus being a wider attack against multiple banks or infrastructure. If the North Korean's objective was to do the maximum damage and have the greatest disruption on the South Korean economy, they could have also launched DDoS attacks against other economic targets, even if they did not have the internal system access at other banks to do more destructive attacks. I therefore deduced a narrow primary objective of disrupting Nonghyup bank. North Korea will never pass up the opportunity to embarrass South Korea as well so I set that as a secondary objective.

---

[23] British Broadcasting Corporation, "North Korea 'behind South Korean bank cyber hack'," *BBC*, 3 May 2011. http://www.bbc.co.uk/news/world-asia-pacific-13263888.
[24] BBC, "North Korea 'behind South Korean bank cyber hack'."
[25] Yonhap News Agency, "N. Korea claims Seoul making up stories to raise tension," *Yonhap*, 4 May 2011. http://english.yonhapnews.co.kr/national/2011/05/04/91/0302000000AEN20110504010700315F.HTML.

North Korea was very successful in their objective to disrupt Nonghyup bank. On 12 April 2011, about half of the servers at Nonghyup bank crashed which resulted in approximately 30 million people who were unable to make online financial transactions or use the bank's ATMs.[26] The attackers launched the attack by implanting the weapon onto a Nonghyup subcontractor's laptop.[27] When the employee connected the laptop to the bank's network, the weapon implanted itself quietly throughout the network and waited for a preset triggering time. According to South Korean official Kim You-Kyung, when the weapon activated, it attempted to destroy the entire server system.[28] Some portions of the bank retained functionality and the defenders mitigated the attack over time, but overall the North Koreans were very successful in their attempt to disrupt the bank. Accordingly, I set $S_1 = 0.80$.

The North Koreans were also more successful against their secondary objective of embarrassing the South Korean government than they had been in the past. This attack received far more press attention and focus by the South Korean people than previous attacks. This attack affected slightly more than half of the population of South Korea, which stands at approximately 50 million. However, as the South Koreans mitigated the attack fairly quickly, it did not set up a "Watergate" type inquiry or bring down any politicians or the government of South Korea. I therefore coded $S_2 = 0.50$.

[26] Mauro, "Major North Korean Cyber Attack on South."
[27] Yonhap News Agency, "S. Korea seeks int'l cooperation for further probe into cyber attack on bank." *Yonhap*, 15 May 2011. http://english.yonhapnews.co.kr/national/2011/05/15/25/0301000000AEN20110515002500320F.HTML.
[28] Finextra, "South Korean bank hit by cyber-attack." *Finextra*, 20 April 2011. http://www.finextra.com/News/Fullstory.aspx?newsitemid=22486.

Since the North Koreans directed this attack specifically at Nonghyup bank without additional DDoS attacks that were clearly within the North Koreans' capability, I gave more weight to the bank objective. If the primary purpose of the attack was to embarrass the South Korean government, North Korea could have added additional DDoS attacks, which would have increased the pressure considerably. Therefore, I weighed the bank objective as four times the weight of embarrassing the South Korean government. I set $W_1 = 0.80$ and $W_2 = 0.20$. The offensive inputs are in table 22.

Table 22 – North Korean Offensive Objectives in 2011 Bank Attack

	Objective	Level of Success (S)	Weighting Factor (W)
1	Disrupt Nonghyup Bank	0.80	0.80
2	Embarrass South Korean government	0.50	0.20

These inputs give a respectable $OCSI_{North\ Korea} = 0.74$, which is the second highest among the eight case studies. South Korea did not attack any North Korean systems so $OCSI_{South\ Korea} = 0.00$.

Level of Functionality (L) and Criticality (C) in North Korean 2011 Bank Attack

The second step in determining cyberspace superiority is to examine the ability of the systems under attack to continue functioning. The attackers did significant damage to Nonghyup bank who lost half their servers in the initial attack. 30 million account holders were unable to access their accounts for three days and 310,000 customers filed

complaints with 1000 demanding compensation.[29] Some aspects of the Nonghyup system did manage to continue operation, but I coded the overall system as minimally functional, which gives $L_1 = 0.20$.

Since Nonghyup bank was the only institution to come under attack, the system criticality is simple at $C_1 = 1.00$. The defensive inputs are in table 23.

Table 23 – Critical South Korean System in 2011 Bank Attack

	System	Level of Functionality (L)	System Criticality (C)
1	Nonghyup Bank	0.20	1.00

These inputs yielded a $DCSI_{South\ Korea} = 0.20$. North Korean systems did not come under attack and so $DCSI_{North\ Korea} = 0.00$.

Relative Cyberspace Superiority Index in North Korean 2011 Bank Attack

North Korea does not rely nearly as heavily on cyberspace as South Korea so $R_{North\ Korea} = 0.05$ and $R_{South\ Korea} = 0.95$. All of these inputs give:

$OCSI_{North\ Korea} = 0.74$
$DCSI_{North\ Korea} = 0.00$
$R_{North\ Korea} = 0.05$
$OCSI_{South\ Korea} = 0.00$
$DCSI_{South\ Korea} = 0.20$
$R_{South\ Korea} = 0.95$

$CSI_{North\ Korea} = 0.70$ and $CSI_{South\ Korea} = 0.19$, which yields:

$RCSI_{North\ Korea} = 0.51$
$RCSI_{South\ Korea} = -0.51$

[29] Finextra, "South Korean bank hit by cyber-attack."

This case is the first attack where North Korea successfully established a high level of cyberspace superiority. They were fundamentally successful in disrupting Nonghyup bank and dominating the news cycle in South Korea, thus successfully embarrassing the South Korean government. It is worthwhile noting that, while the attack was very successful, the South Koreans were able to mitigate it quickly and had restored most of the functionality at the bank after three days.

North Korea versus South Korea April 2013 Attack

Two years after the 2011 bank attacks, the North Koreans attacked again, this time against a broader target set during a time of heightened tensions. Analysts called these attacks the Dark Seoul attacks.

Level of Success (S) and Weighting Factor (W) in North Korean April 2013 Attack

As before, the first step in determining who had how much cyberspace superiority is to determine the identity of the attacker. The same discussion earlier about attribution to North Korea applies, they denied any involvement but the circumstantial evidence is strong enough for me to attribute the attack to them anyway. McAfee had a team do extensive research of the Dark Seoul attacks and uncovered a covert espionage campaign called Operation Troy that linked all of the previous attacks to North Korea.[30] North Korea had also identified the specific broadcasters hit as potential targets, and "According to InformationWeek, the hacker responsible for the attack inadvertently exposed his or her IP address for a few minutes because of a technical problem. That address has been identified as being registered to the only Internet service provider in

[30] Sherstobitoff and Liba, "Dissecting Operation Troy: Cyberespionage in South Korea," 28.

North Korea."[31] On top of that, in the international relations environment, South Korea was in the middle of a set of major exercises condemned by North Korea in a time of rising tensions. The evidence of attribution of the attack to North Korea is significant enough for this study.

To determine the North Korean objectives, I first examined their targets. Dark Seoul targeted three television broadcasters, YTN, MBC and KBS as well as three banks, Shinhan, Nonghyup, and Jeju as well as the telecommunications operator LG U+.[32]

The type of attack also provides evidence of what the attackers were seeking. Dark Seoul was very destructive and the attacker erased the master boot records of the 48,000 computers infected. The attacker also utilized other techniques clearly intended to affect both Windows and Linux systems to broaden the attack's effects as much as possible.[33]

Based on Dark Seoul's targeting, the first objective of the North Koreans was to disrupt the South Korean banking system. However, Dark Seoul's bank attacks were only minimally successful. Some services were temporarily blocked, but restored after two hours, while some banks under attack suffered no damage at all.[34] I therefore set $S_1 = 0.20$.

---

[31] Thawte, "Cyberattack Traced to North Korea," *Thawte*, 2013. http://www.thawte.com/about/news/?story=423684.
[32] Japmarpaung, "Dark Seoul – Postmortem," 3 May 2013. http://japmarpaung.com/2013/05/03/dark-seoul-postmortem/.
[33] Japmarpaung, "Dark Seoul – Postmortem."
[34] Choe Sang-Hun, "Computer Networks in South Korea Are Paralyzed in Cyberattacks," 20 March 2013. http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html.

The attacks against the broadcaster's computer networks were more successful although they did not force any of the stations off the air. The broadcasters however, lost most of their internal networks so I set $S_2 = 0.50$.

While there was some negative press in South Korea but the government did not end up looking weak or incompetent as they aggressively responded to the attacks and reconstituted the networks fairly quickly. As a result, I also set $S_3 = 0.50$ to represent approximately half success against the objective of embarrassing the South Korean government.

McAfee's theory that the attackers intended to destroy evidence from Operation Troy is intriguing, although it is difficult to code its success.[35] Security researchers discovered Operation Troy, but its connection to Dark Seoul was no discussion outside of Internet security circles in the broader media. I therefore set $S_4 = 0.50$ as half-success.

I considered disrupting the banks and broadcasters as the primary purpose of the attackers based upon their target set. Therefore, I assigned each of those objectives equal weight, and gave each four times the weight of the remaining two objectives of embarrassing the South Korean government and erasing Operation Troy. The offensive inputs are in table 24.

[35] Sherstobitoff and Liba, "Dissecting Operation Troy: Cyberespionage in South Korea," 28.

Table 24 – North Korean Offensive Objectives in April 2013 Attack

	Objective	Level of Success (S)	Weighting Factor (W)
1	Disrupt Banks	0.20	0.40
2	Disrupt Broadcasters	0.50	0.40
3	Embarrass South Korean Government	0.50	0.10
4	Erase Evidence of Espionage	0.50	0.10

These inputs give an $OCSI_{North\ Korea} = 0.38$, which is around the mid-range of the eight case studies I examined. South Korea had no offensive objectives and so $OCSI_{South\ Korea} = 0.00$.

Level of Functionality (L) and Criticality (C) in North Korean April 2013 Attack

The next step in calculating the level of cyberspace superiority is to determine the defensive inputs for the model. There were two systems that South Korea was trying to defend, the banks and the media companies.

The banks were quite successful in defending their systems and only experienced minimal disruption. Some banks that North Korea attacked reported no damage, while other banks were back in operation after two hours.[36] Therefore I set $L_1 = 0.80$.

On the media side, the broadcasters lost their internal networks but the attackers were unable to take them off the air. This represents a middle ground and so I set $L_2 = 0.50$. The defended systems are in table 25.

[36] Sang-Hun, "Computer Networks in South Korea Are Paralyzed in Cyberattacks."

Table 25 – Critical South Korean Systems in April 2013 Attack

	System	Level of Functionality (L)	System Criticality (C)
1	South Korean Banking Systems	0.80	0.75
2	South Korean Media Internal Systems	0.50	0.25

This coding gives a $DCSI_{South\ Korea} = 0.73$. Since North Korea was not attacked, $DCSI_{North\ Korea} = 0.00$.

Relative Cyberspace Superiority Index in North Korean April 2013 Attack

North Korea does not rely nearly as heavily on cyberspace as South Korea so $R_{North\ Korea} = 0.05$ and $R_{South\ Korea} = 0.95$. All of these inputs give:

$OCSI_{North\ Korea} = 0.38$
$DCSI_{North\ Korea} = 0.00$
$R_{North\ Korea} = 0.05$
$OCSI_{South\ Korea} = 0.00$
$DCSI_{South\ Korea} = 0.73$
$R_{South\ Korea} = 0.95$

$CSI_{North\ Korea} = 0.36$ and $CSI_{South\ Korea} = 0.69$, which yields:

$RCSI_{North\ Korea} = -0.33$
$RCSI_{South\ Korea} = 0.33$

North Korea did not achieve the same level of cyberspace superiority that they did in the bank attacks of 2009. This situation was due to apparent improvements in the South Korean capacity to mitigate, repair, and reconstitute. South Korea has chosen to take national cyberspace defense very seriously and has poured significant resources into this domain. The North Korean attacks have trended to be more effective over time, but the South Korean defenses have improved as well. In this case, the South Koreans were

able to keep the North Koreans from gaining cyberspace superiority. This sequence of attacks by North Korea on South Korea shows that the offense does not have an insurmountable advantage over the defense. A prepared defender can defeat even sophisticated attacks.

APPENDIX C – DESCRIPTION OF CYBERSPACE TOOLS

The purpose of this appendix is to present basic descriptions of the tools and techniques referenced in the main body of this analysis. I grouped the tools and techniques as cyberspace means, cyberspace ways, defensive blocks, and counters to defensive blocks. All of these elements are in figure 18.

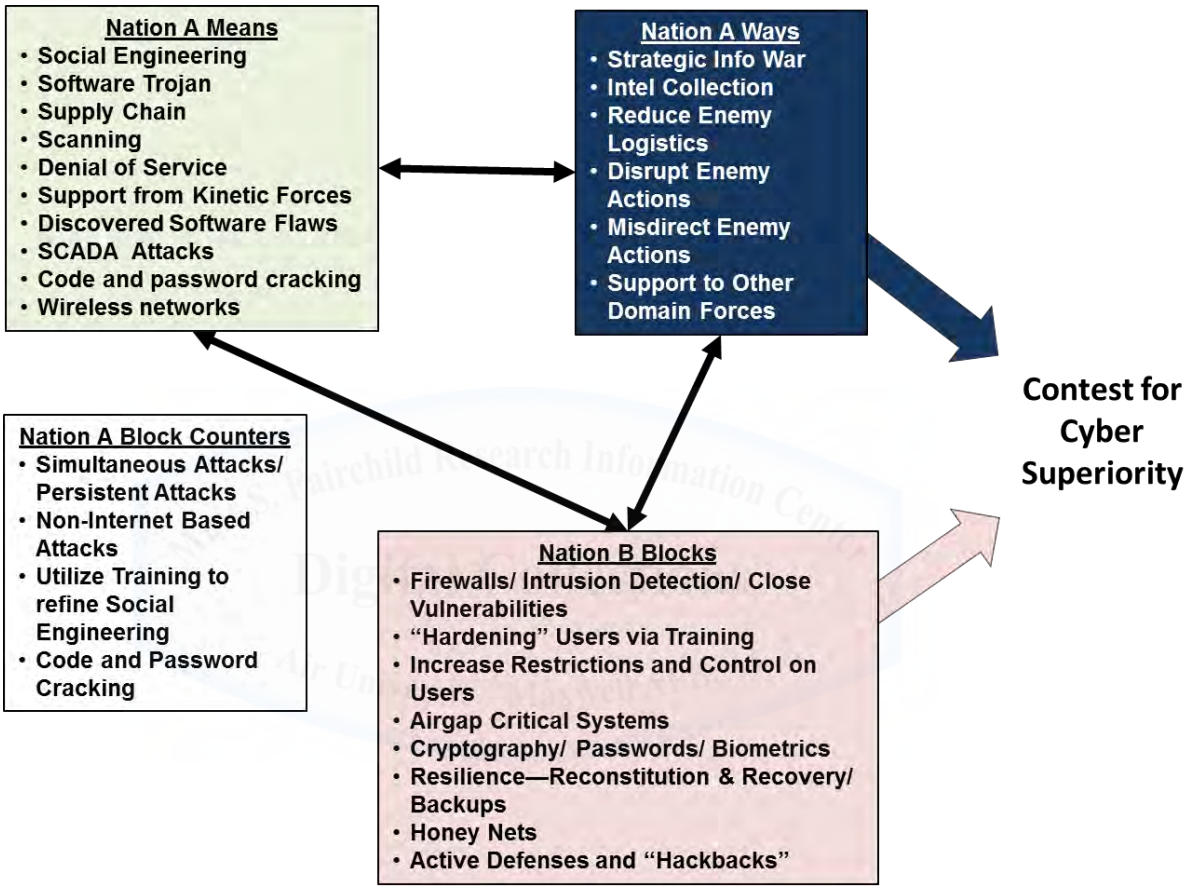

Figure 18 – Cyberspace Conflict Elements
Source: Author's Original Work

I also use this diagram in the case studies in chapter 5 as a way of quickly identifying which elements were active in a particular case. The first tools I will describe are the means available to cyberspace attackers.

Cyberspace Means

Cyberspace means are the tools that a combatant can use in cyberspace to accomplish his or her objectives. Some of the tools have evolved rapidly, but the categories of tools have not. For example, Distributed Denial of Service (DDoS) attacks evolved from simpler Denial of Service (DoS) attacks, but what they are attempting to do to the targeted system remains the same. There is a continuous refinement of the tools, but only rarely does an entirely new category appear.

The means available to an attacker in cyberspace are not completely separate and distinct. At times they can blend together and one tool may be required for the action of another. For example, scanning may reveal an opening that an attacker can utilize via a discovered software flaw to implant a software Trojan. All three tools were required to make the overall attack happen. In a normal cyberspace attack, an attacker collects intelligence on the target to identify an opening, and then the attacker exploits the opening to insert a payload and accomplish some action.

Social Engineering

The first important cyberspace means is social engineering or the use of psychological manipulation to trick a user into providing access into a system for an attacker. This manipulation is usually the most effective method of gaining access into an enemy system. A famous hacker, Kevin Mitnick has said,

> A company can spend hundreds of thousands of dollars on firewalls, intrusion detection systems and encryption and other security technologies, but if an attacker can call one trusted person within the company, and that person complies,

> and if the attacker gets in, then all that money spent on technology is essentially wasted.[1]

Social engineering is probably the most utilized and effective method of attacking computer systems and networks today, and it is very hard to defend against because if one person says no, the attacker can keep going down the phone list until he or she finds someone more gullible.

There is no "patch" for social engineering according to O'Harrow, "Social engineering works because it targets a vulnerable part of cyberspace that cannot be patched with technical fixes: human beings."[2] As the most common means utilized by cyberspace attackers, social engineering plays an important role in cyberspace superiority and sometimes opens the door for the second means of attack in cyberspace, software Trojans.

Software Trojan

A second means used in cyberspace superiority is software Trojans that rely on inserting secret "back doors" into software to provide an attacker access into a defended system. According to Homer, the Greeks attacking Troy could not get into the city, so cunning Ulysses hatched a plan to sneak soldiers into the city inside a large wooden horse that the Trojans would think was a statue honoring the Greek gods. Once the Trojans brought the horse into the city, the Greeks snuck out, opened the gates to their forces outside and took the city. This story is an excellent analogy of how a "software Trojan"

[1] Cable News Network. "A convicted hacker debunks some myths," *Cable News Network*, 13 October 2005. http://www.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/.
[2] O'Harrow, *Zero Day*, Kindle Location 600, part 4.

works. While social engineering relies on tricking a human into opening a door, software Trojans accomplish the same thing through malicious code inserted into trusted software.

The complexity of modern software makes it easier for attackers to insert back doors. Software has become increasingly complex and some operating systems such as Windows Vista have in excess of 50 million lines of code. When you include the fact that the industry average for errors per 1,000 lines of code is 15-50, there are a tremendous number of mistakes in every piece of software running on any computer.[3] Software Trojans rely on hiding inside the massive number of lines in modern code and the difficulty in debugging them. Attackers can emplace these access points when the authors write the code, or attackers can plant them in the code through access provided by social engineering or other techniques and then utilize them to access systems running the modified software. Most modern systems utilize firewalls, which automatically block incoming access requests but allow computers inside the firewall to establish connections outside. A simple software Trojan will "phone home" and open an access point through the defenses, which gives the attacker a way in. Software Trojans are widely used by nation states with significant cyberspace resources and are important elements of cyberspace superiority. Software Trojans are like a traitor inside a castle under siege who opens a side door to the enemy. Unfortunately for defenders, software Trojans are not the only potential traitors inside the walls.

[3] Steve McDonnell, *Code Complete*, 2nd Ed, (Redmond WA: Microsoft Press, 2004), Quoted by Hans von Storch at http://klimazwiebel.blogspot.com/2011/07/coding-errors-how-many-errors-are-on.html.

Supply Chain Attacks

Another major means of implanting access ports into a combatant's systems to gain cyberspace superiority is through supply chain attacks. According to the Comprehensive National Cybersecurity Initiative ordered by President Obama, "Globalization of the commercial information and communications technology marketplace provides increased opportunities for those intent on harming the United States by penetrating the supply chain to gain unauthorized access to data, alter data, or interrupt communications."[4] This threat may have already manifested itself in kinetic combat, there has been speculation that the Israelis caused the Syrian radar system's mysterious failure, precisely timed to coincide with an Israeli airstrike on the Syrian nuclear facility through this type of hardware supply chain attack.[5] The United States is attempting to find reliable methods of discovering hardware "trap doors" but with the number of transistors and complexity of chips, it is increasingly difficult to do.[6] A new Xbox One video game has five billion transistors; a complex defense related network will have far more and the government purchases the majority of its equipment as Commercial off the Shelf (COTS) components that could have made under less than stringent control of suppliers or even by an adversarial country. This avenue is most open to combatants seeking cyberspace superiority who have significant electronics design or manufacturing sectors such as the U.S. and China. If an attacker is not able to

[4] White House, "The Comprehensive National Cybersecurity Initiative," Accessed on 30 August 2013. http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.
[5] Sally Adee, "The Hunt for the Kill Switch," *IEEE Spectrum*, 2008. http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0.
[6] DARPA is studying this problem via their Trusted Integrated Circuits (TRUST) program but has not released any results.

implant a trap door on the inside, there is the opportunity to find a chink in the armor on the outside via scanning.

Scanning

While supply chain attacks require a high level of technical sophistication, port scanning is available to cyberspace attackers at all levels. Port scanning is largely responsible for the gigantic number of "cyberspace attacks" reported in the media.[7] To use the airpower domain as an analogy, these "attacks" are not blowing up factories, they are attempted penetrations of airspace to see if the adversary notices, to figure out how good his defenses are, and where there are gaps. Every network can have thousands of "ports" or openings to the outside. Normally, firewalls keep the vast majority closed unless they are in use by a legitimate program. The problem is that given the complexity of modern networks, often the defender accidentally leaves a door open that he or she should have closed. An attacker can "scan" across all the possible ports to see if there are any open that he can exploit. This scanning is extremely easy to do and there is free software on the web that will accomplish port scans, which is one of the reasons why there are so many "attacks." Finding an open port is only the first step; an attacker who intends to achieve a useful level of cyberspace superiority has to do more. Exploiting an open port requires a greater level of skill and the ability to utilize a service behind that port on the target computer system to accomplish the attacker's objectives.

[7] Belk and Noyes, "On the Use of Offensive Cyber Capabilities," 19.

Denial of Service

Cyberspace attackers without the skill or resources required to break into systems can still attempt to damage an enemy by attempting to deny the ability of his systems to communicate. These types of attacks are much easier to execute than actually breaking into an enemy system and modifying information. A denial of service attack is a method of blocking access to some Internet enabled service or database, such as a web page. The attacker simply requests the page to supply information over, and over, and over at such a volume that the attacked system cannot keep up, which blocks access to the real users. If the attack is coming from one address or one region, it is relatively simple to block by instructing the defending computer to ignore requests from those addresses.

To get around IP address exclusion defenses, the most common method of executing a denial of service attack today is a Distributed Denial of Service attack (DDoS) where the attacker does not use his or her own system, but instead uses a network of computers under his or her control. These are normally computers owned by private individuals, who through poor computer security practices have had their computers turned into "zombies" or "bots", which are secretly controlled by a "bot-herder". To the owner of the computer, there is nothing to indicate they are no longer in control of their machine as it still seems to work normally, if perhaps a bit slower. Behind the scenes, the "bot-herder" can use their computer to target a combatant's networks as part of a DDoS. These botnets are part of organized cyberspace crime's basic business model and anyone can rent them for a small fee; as of 2010, the average

price was $9 an hour.[8] During the attack on Estonia in 2007, "The 10 largest assaults blasted streams of 90 megabits of data a second at Estonia's networks, lasting up to 10 hours each. That is a data load equivalent to downloading the entire Windows XP operating system every six seconds for 10 hours."[9] It is important to note that these attacks can go well beyond not being able to access a website. There is no technical reason why an attacker could not use DDoS against any system connected to the Internet such as a logistical database that would have far more serious operational impact and these types of attacks are hard for defenders to address due to the "innocent" character of the attacking computers.

DDoS attacks have proven difficult for nation states to deal with as disabling the attacking computers involves disabling neutral "civilian" computers whose owners are unaware they are being used in cyberspace warfare. Several of the attacks I examined in the case studies involved these sorts of attacks where governments had to decide whether to disable the attacking computers. If the attacking computers are located in neutral countries, the political costs of doing so will normally be prohibitive, and the computers selected for attacks will normally be in nations that have better Internet connectivity. In at least one case, the South Koreans did decide to disable attacking computers, but that decision only applied to the machines within South Korea.[10] If denial of service attacks are on the low end of brute force cyberspace means to seek cyberspace superiority, then kinetic warfare represents the high end.

---

[8] Dancho Danchev, "Study finds the average price for renting a botnet," *ZDNet*, 26 May 2010. http://www.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528.
[9] Andrew P. Hansen, "Cyberflag: A Realistic Training Construct," (Master's Thesis, Air Force Institute of Technology, 2008), 12.
[10] Jane Han, "Cyber Attack Hits Korea for Third Day."

Support from Kinetic Forces

Because the assets that produce cyberspace exist in the physical world, physical attacks against these assets with kinetic forces are an important means that nation states can utilize in seeking local cyberspace superiority. In the midst of a kinetic conflict, the most effective cyberspace weapon may be a 2000lb bomb dropped on a telecommunications hub or control center. Physical destruction is much harder to repair than simply reloading software from a backup and an attack does not have to be as blatant as a bomb from above. Communications officers already live in fear of innocent backhoes; not-so-innocent targeted backhoes can do even more damage if an attacker severs the right cables. The only limit on the number of ways to disrupt networks through attacking their physical components is the imagination and resources of the attacker.

The linkage between cyberspace and the physical world provides an attacker's best opportunity to attack an enemy's offensive cyberspace capabilities through offensive counter cyberspace. Some authors, such as Butler, do not think that offensive counter cyberspace is a useful concept but is instead a doctrinal bleed over from the air domain where it does have applicability.[11] I agree that offensive counter cyberspace is most likely not a useful concept if you restrict the discussion to cyberspace weapons. However, if you broaden the scope to include the other physical domains, there is much more potential utility. If a combatant is able to identify the main operations center from which the adversary is launching attacks and physically destroy it, killing many of the

[11] Butler, "Refocusing Cyber Warfare Thought," 52.

personnel; that could be a tremendously effective offensive counter cyberspace attack akin to destroying an enemy fighter airfield as an offensive counter air attack. This type of physical attack can affect not only local, but also universal cyberspace superiority if an attacker can find and attack the enemy's universal cyberspace assets.

Discovered Software Flaws

A critical means through which cyberspace attackers pursue their objective in cyberspace is discovered software flaws. As noted previously, software flaws are extremely common given the large numbers of lines of code and attackers can often easily exploit these flaws due to the characteristics of computers. Libicki helps explain why these flaws create vulnerabilities when he says, "What helps slip attackers past guards is that the control systems of cyberspace are complex, arcane, generally opaque, and brittle. They do not react well to the unexpected—which is to say, conditions for which they are not specifically programmed."[12] One example is a "buffer overflow." Essentially, an attacker deliberately writes information past what is legitimate in response to a query and if the defending computer does not catch it, the attack writes that information directly into memory. Then the attacked system interprets the overflow as legitimate code and executes it. Software companies attempt to patch vulnerabilities that they know about, but they can do nothing to deal with the ones that they do not know about.

Software flaws known only to the attacker are the "crown jewels" of a cyberspace attacker's arsenal. These vulnerabilities are referred to as zero-day attacks, because the

[12] Libicki, *Conquest in Cyberspace*, 33.

timer on the vulnerability starts at zero when the first attack is made and then increments up day by day as software engineers scramble to develop a patch. Defenders who are unaware of the specific vulnerability rely on scanners looking for generic signatures that often have only moderate success. That is why zero-day exploits are so important and guarded so carefully when discovered. There is even a market in zero-day vulnerabilities with a Window's vulnerability selling for $60,000 to $120,000 and an iOS vulnerability going for $100,000 to $250,000.[13] According to Carr, targeted zero day attacks are the most powerful weapons available to offensive cyberspace operators.[14] It is important to note that just because the defender knows about a vulnerability, it does not automatically follow that the defender has properly patched the particular system under attack. A system administrator can inadvertently leave a vulnerability open well after a patch has been developed and issued if he or she does not keep the entire network up to date, which can be an overwhelming task on a large network. If zero-day discovered software flaws are the crown jewels, SCADA attacks represent the cyberspace version of heavy artillery that can do the most damage.

SCADA Attacks

The cyberspace means with the greatest current potential to alter a nation state's decision-making is attacks on Supervisory Control and Data Acquisition (SCADA) systems. Attacking utilizing this means can have the greatest strategic payoff for an attacker. SCADA systems are the unseen heroes of our modern industrial society and

[13] Andy Greenberg, "Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits," Forbes, 23 March 2012. http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.
[14] Carr, *Inside Cyber Warfare*, Kindle location 3562, chap. 10.

operate infrastructure such as power plants, dams, water treatment facilities, etc., but have important vulnerabilities. The largest problem is that when most of these systems were developed, there was no need for security and so developers did not design it in. Most SCADA systems were "stand alone" and not connected to the Internet so to implant malicious code would have required an attacker to access a physically secured facility and directly connect to the control system. However, in the interest of efficiency, many utility companies connected their SCADA systems to the Internet to allow for better monitoring and updating so now anyone can access all those connected systems worldwide. Many of these SCADA systems still have no real security and companies and governments are scrambling to catch up and put some security on the vulnerable systems. To make things easier for attackers, there is a "Google for hackers" that provides a search engine for vulnerable SCADA systems.[15] Attackers have shown that even systems that are "air gapped" and in high security areas are still vulnerable.

There are numerous examples of attackers getting into SCADA systems. At its heart, Stuxnet was a SCADA attack used by an attacker to cause the physical destruction of centrifuges while reporting that all was well to the system's engineers.[16] There have also been successful SCADA attacks against power grids, water plants, gas pipelines and many other types of infrastructure.[17] According to Robert Miller and Daniel Kuehl, the four types of infrastructure most vulnerable include systems that deal with electricity,

[15] Naraine, Ryan, "Shodan search engine exposes insecure SCADA systems," *ZDNet*, 2 November 2010. http://www.zdnet.com/blog/security/shodan-search-exposes-insecure-scada-systems/7611.
[16] Belk and Noyes, "On the Use of Offensive Cyber Capabilities," 8-9.
[17] Peritz, and Sechrist, "Protecting Cyberspace and the US National Interest," 8.

communications, money and transportation. Disruption of those systems would quickly cause societal confusion and disorder.[18]

Recovering from a SCADA attack may not be as simple as resetting a system and turning back on the things that an attacker turned off. The Aurora test demonstrated that an attacker could physically destroy a generator through cyberspace by sending malicious commands.[19] Generators are not the only physical devices that attackers could theoretically damage through SCADA attacks; an attacker could damage almost any computer-controlled item. Attackers can order chips to do continuous work, while the attacker disables cooling systems to produce hardware failure, attackers can order actuators past their physical stops burning out motors, and the designers of Stuxnet could order nuclear centrifuges to spin erratically causing failure.

While many SCADA systems are vulnerable, access into the system does not automatically translate into the ability to destroy it. Generating physical damage requires deep understanding of how a designer has configured a system. Fortunately, most hackers have proven unable to accomplish more than nuisance SCADA attacks, such as dumping some sewage. Unfortunately, nation states do have the knowledge and resources required to translate SCADA access into more significant physical effects. SCADA attacks represent what may be the most important means to cyberspace attackers, and also the area most in need of aggressive defense from cyberspace defenders. In a significant nation state conflict, SCADA systems will be a key battleground of cyberspace superiority. While the fight over SCADA enabled

[18] Robert A. Miller and Daniel T. Kuehl, "Cyberspace and the 'First Battle' in 21stcentury War," *Defense Horizons* 68, (2009): 2.
[19] Shakarian, et al., *Introduction to Cyber-Warfare*, Kindle Location 6561, chap. 12.

infrastructure will be out in the open, behind the scenes another cyberspace means will be quietly at work.

Code and Password Cracking

An important cyberspace means that will allow an attacker to execute many of the other types of attacks is the ability to break passwords and codes. Many systems now utilize encrypted data and while it is easier to get someone to give you their password through social engineering and pretending to be tech support, code and password cracking will sometimes be required. In general, those who properly encrypt their data have the advantage right now, and barring significant changes in the computing environment such as the development of quantum computing, they are likely to maintain the advantage. Fortunately for attackers, humans run the encryption schemes and often make mistakes. Even "unbreakable" encryption can be broken through exploiting human errors. Common errors include weak passwords such as "password," using the same password on multiple systems, and poor physical control of written down passwords. Lifting up the keyboards in most any large office environment will likely still produce a good number of written down passwords, even today when people should know better. Breaking access codes can also facilitate attacking systems via wireless networks.

Wireless Networks

Wireless networks represent a way for an attacker to break into a defended system that bypasses many of the defenses. Wireless networks have become almost ubiquitous from coffee shops to corporate boardrooms but come with some significant security vulnerabilities that some defenders do not fully appreciate. To a network, someone who has connected via wireless often looks like someone who is "inside" and thus they are

already inside the first lines of defense of firewalls and intrusion detection systems. According to O'Harrow, anyone who comes into a facility with a wireless device can often connect to the network through "osmosis" and bypass most of the defenses.[20] However, with the proper equipment, a combatant may not have to send anyone into the facility.

Attackers can use larger, more focused antennas to achieve a connection despite being well outside of what defenders would normally expect. The wireless antennas most people use in cellular phones and laptops are miniscule and the physics of antennas limits their range. Commercially available antennas can produce ranges of several miles with a clear line of sight. The current record for a Wi-Fi connection is 238 miles, although that of course was with very large, specialized equipment.[21] Now that I have examined the most common means utilized by attackers in cyberspace, it remains to turn next to the things that an attacker can do with those means in pursuit of cyberspace superiority.

Cyberspace Ways

An attacker is able to achieve offensive cyberspace superiority when he can connect his cyberspace means and his cyberspace ways to achieve his operational objectives in cyberspace. A defender achieves defensive cyberspace when he is able to protect his systems and block the attacker from achieving his objectives.

Dominance of cyberspace is useless if a combatant cannot translate that dominance into concrete gains that enable the combatant's strategists to connect

[20] O'Harrow, *Zero Day*, Kindle Location 304, part 2.
[21] Michael Kanellos, "New Wi-Fi distance record: 382 kilometers," *CNet*, 18 June 2007. http://news.cnet.com/8301-10784_3-9730708-7.html.

successfully means, ways, and ends. According to Libicki, "If control, influence, or competence in the medium has little to do with the delivery of military power in the more conventional realms, then no one would need it except perhaps for bragging rights."[22] Fortunately for cyberspace operators, cyberspace superiority does deliver military power in the conventional realms through the ways we will next explore.

Strategic Information Warfare

The first way that an attacker can utilize in cyberspace to deliver military power is through strategic information warfare, which is an unfortunate name for several reasons. First, while there are many different definitions of strategic, its use in "strategic information warfare" tends to obscure rather than illuminate. If strategy is connecting domain ways and policy ends, what is "strategic" about strategic information warfare? It is a tool used by attackers to execute a strategy, not a strategy itself. In some ways, the confusion in the term is similar to the confusion over "strategic bombing" which once again is a tool, not a strategy. If strategic information warfare is not strategic, then what is it?

Analysts have given many different definitions of strategic information warfare. RAND is largely responsible for the widespread use of the term strategic information warfare out of a 1996 study and I will start with their definition. Strategic information warfare is, "wherein nations utilize cyberspace to affect strategic military operations and inflict damage on national information infrastructures."[23] The limitation to this definition

[22] Martin C. Libicki, "Military Cyberpower." in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, DC: Potomac Books, 2009), 275.
[23] Roger C. Molander, Andrew S. Riddile and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, CA: RAND, 1996), 1.

stems from its 1996 date, when analysts did not yet consider the concept of striking anything in the physical domains through cyberspace so the RAND definition is not as complete as the definitions of some later analysts.

Lonsdale offers that strategic information warfare bypasses enemy surface forces to affect directly an enemy center of gravity.[24] Lonsdale's definition is more useful because it focuses more broadly on affecting a center of gravity directly through cyberspace. Lonsdale's definition is similar to that of Eric Trias who said that, "The goal of strategic attack is to apply force systematically against enemy centers of gravity in order to produce the greatest effect for the least cost in dollars and lives."[25] Lonsdale and Trias' definitions are useful, but I find it more useful to bound strategic information warfare not only by the domain, but also by its objectives.

I define strategic information warfare as actions by an attacker through cyberspace to produce an effect that changes the defender's decision-making calculus in a way favorable to the attacker. This definition deliberately excludes brute force methods and relies on military coercion to bring the enemy to choose to submit to an attacker's demands.

Cyberspace attackers should focus strategic information warfare on coercion instead of attempting brute force attacks, which are unlikely to be effective in the cyberspace domain. There are two basic paths to success for attackers in any domain, the enemy can choose to accept the attacker's demands, or the attacker can deprive the enemy of any means to resist. Genocide and the capture of the enemy's territory without

[24] Lonsdale, *The Nature of War in the Information Age*, 135.
[25] Eric D. Trias and Brian M. Bell, "Cyber This, Cyber That…So What?" *Air Space Power Journal* Volume 24, no. 1 (2010): 91.

surrender are examples of brute force methods. When the Ottoman Turks captured Constantinople in 1453, there was no surrender, and while numerous individual Byzantines survived, they had lost any organized ability to resist. Because people live in the land domain, it is extremely unlikely that any conceivable attack based in cyberspace could completely remove a nation's ability to resist. If the United States destroyed every computing device in North Korea, while simultaneously disrupting all North Korean infrastructures, the North Koreans could still resist, albeit with less effectiveness. Because the North Koreans would still have options and choices available to them, strategic information warfare will have to rely on coercion. Because of the similarities between strategic information warfare and strategic bombing, the air domain provides a good template to look at strategic information warfare.

In *Bombing to Win*, Pape develops three strategies of military coercion that an attacker can use to attempt to change the decisions made by a defender.[26] The first of these strategies is punishment, which attempts to raise the societal cost to the defender, normally through inflicting suffering. The second strategy is risk, which is a modulated form of punishment that threatens further suffering if the defender does not comply with the attacker's demands. The final strategy is denial, in which the attacker targets the defender's military ability to achieve his objectives.[27] An attacker could execute each of these strategies from cyberspace with cyberspace superiority. For example, an attacker could utilize a punishment strategy and shut down the enemy's power grid. That same attacker could instead use a risk strategy and shut down one small section of the enemy

[26] Pape, *Bombing to Win*, 19.
[27] Pape, *Bombing to Win*, 19.

power grid as a demonstration that he can shut down the rest if the defender does not comply with his demands. Finally, the Stuxnet attack is an example of denial, where the attacker attempted to prevent the defender from achieving the defender's objectives, in this case through destroying the centrifuges Iran was utilizing to make the material for nuclear weapons. Pape's analysis of these three strategies in the airpower domain also has utility when looking at the cyberspace domain.

In the air domain Pape found that coercion could work, but only if the concessions sought by the attacker are relatively unimportant to the defender.[28] After looking at 40 cases of attempted coercion in the air domain, Pape found that denial strategies had the best chance of success.[29] Punishment strategies had a low probability of success, and risk strategies fared even worse as a weaker form of punishment. It is reasonable to assume that these same findings are likely to apply in cyberspace conflict as well. The mechanism of weapon delivery is different, but the heart of coercion lies in the decision-making processes and psychology of the defender, not in the specifics of how pressure is applied. This analysis suggests that cyberspace operators would do well to be cautious when predicting how likely strategic information warfare is to cause the enemy to concede on important issues.

Since physical destruction of targets and infrastructure by high explosives was normally insufficient to induce nations to surrender their war aims, it seems unlikely that cyberspace attacks will prove more effective. Lonsdale captures this circumstance well when he says that, "The notion that a population, or state, would surrender as a result of

[28] Pape, *Bombing to Win*, 20.
[29] Pape, *Bombing to Win*, 20.

its electricity or banking system going down in the face of SIW [Strategic Information Warfare] is difficult to accept in light of the experience of strategic bombing."[30] One of the key reasons why punishment has often been disappointing is that the enemy gets to decide when he has had enough, and historically that "enough" has often been higher than the attacker thought it would be.[31] Strategic information warfare can provide an important tool in the toolkit, but attackers should not expect it to be a shortcut to easy victory any more than strategic airpower was.

For coercion via strategic information warfare to succeed, the cyberspace attacks must be more unpleasant than the sacrifice the attacker is asking the defender to make, and it needs to appear that things are going to get worse for him, not better. Clausewitz clearly laid out both of these conditions in his discussion on forcing the enemy to do your will.[32] Unfortunately for strategic information warfare, the characteristics of cyberspace as discussed in chapter 3 most often means that cyberspace attacks will get less severe over time and thus from Libicki, "But can strategic cyberwar induce political compliance the way, say, strategic airpower would? Airpower tends to succeed when societies are convinced that matters will only get worse. With cyberattacks, the opposite is more likely."[33] While strategic information warfare is no more panacea than strategic bombing, it has a role to play in cyberspace conflict and attackers can use it successfully given the right conditions.

[30] Lonsdale, *The Nature of War in the Information Age*, 165.
[31] Lonsdale, *The Nature of War in the Information Age*, 163.
[32] Clausewitz, *On War*, 77.
[33] Libicki, *Cyberdeterrence and Cyberwar*, xv.

Intelligence Collection

A second way that nation states can connect cyberspace means to policy ends is through intelligence gathering and cyberspace espionage. Breaking into an enemy's system to read his war plans, or check on the readiness of his forces or his capabilities are all examples of this type of operation. The importance of cyberspace intelligence in support of other cyberspace operations cannot be overstated. One of the reasons that the United States did not use cyberspace attack in Libya is that there was not time to do the necessary intelligence preparation.[34] There are also several more issues beyond just time.

One issue with cyberspace intelligence is that doing intelligence work can cause the enemy to react in negative ways even if you do not actually intend to attack. Libicki calls cyberspace intelligence gathering "Heisenberg country" because the act of gathering intelligence can change enemy actions much like the observer alters quantum states in physics.[35] Scanning and intelligence work can generate a similar effect to the security dilemma in realist international relations theory. Nation A scans nation B because nation A thinks nation B might be hostile. Nation B was not actually intending to attack but takes nation A's scan an evidence that A is intending to attack so builds weapons to attack nation A. Nation A has generated the very outcome it was trying to avoid. A cyberspace attacker also has to decide whether to use the intelligence collected, or to stay quiet and try to gather more.

The second major issue with cyberspace and intelligence work is that there is often a tradeoff between a successful attack and continuing intelligence. If an attacker

[34] Rosenzweig, *Cyber Warfare*, Kindle Location 805, chap. 3.
[35] Libicki, *Conquest in Cyberspace*, 91.

has developed a successful intrusion into an enemy computer system, he can often both use that intrusion to produce a cyberspace attack, or keep quiet and use the intrusion for intelligence gathering. There is an obvious and automatic tension between operations and intelligence staffs, as the operators will tend to value action and the intelligence professionals continuing intelligence. There is no easy and obvious answer to the dilemma, so an attacker will have to deal with each situation as priorities and senior leaders determine. [36] Despite these tensions, intelligence gathering will remain one of the key ways that cyberspace attackers utilize.

For an attacker to move beyond brute force attacks such as distributed denial of service attacks into more effective types of attacks will require significant cyberspace intelligence collection. As Carr wrote, "A sophisticated attacker aided with intelligence gathered from reconnaissance can execute a devastating attack, whereas an unsophisticated attacker without any intelligence on its targets will be relegated to simple brute-force attacks."[37] An attacker's success in gathering intelligence can make all the difference in cyberspace conflict.

Reduce Enemy Logistics

The third way that cyberspace attackers can connect cyberspace means and ends is through attacking enemy logistical systems. Modern militaries rely on their information systems for logistical support and as multiple users need to access them in various locations, these systems are often on unclassified networks and more open to

[36] Owens, et al., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 156.
[37] Carr, *Inside Cyber Warfare*, Kindle location 4189, chap. 12.

attack. Misdirection that sends supplies to the wrong places, changes inventory information, or alters timetables could have tremendous impact on a campaign, particularly if the enemy is heavily reliant upon moving large numbers of forces in a short period of time a great distance. There is a long history of cyberspace attacks on logistic systems going all the way back to the early 1990s. During Operation Desert Shield, a group of hackers attacked U.S. logistics networks and databases. These attacks delayed the deployment of some elements because logisticians had to re-verify information from the affected databases.[38] This attack will likely not be the last time that cyberspace attackers focus on U.S. logistics.

These types of attacks on logistics are of particular interest to potential foes of the United States. Any nation relying on long or fragile logistical lines of communication is vulnerable to logistics based attacks, even if those lines of communication are internal. However, the United States has historically relied on massive and complex logistical systems to project power. Not surprisingly, the Chinese have shown a special interest in this type of attack and analysts expect them to attempt to attack American transportation, logistics, and command and control networks during a conflict.[39] Although the attacker accomplished the effects with airpower, not cyberspace attack, analysts can see what is possible from the first Gulf War when a lack of supplies completely immobilized Iraqi units.[40] Accomplishing the same immobilization from cyberspace would be more difficult as cyberspace weapons are more likely to be disruptive rather than destructive.

---

[38] Robert A. Miller and Daniel T. Kuehl, "Cyberspace and the "First Battle" in 21stcentury War," *Defense Horizons* 68, (2009): 3.
[39] Carr, *Inside Cyber Warfare*, Kindle location 4015, chap 11.
[40] Luttwak, *Strategy: The Logic of War and Peace*, 196.

While attacking enemy logistics through cyberspace can have utility, disrupting logistical systems will only provide a temporary effect when compared with destroying the supplies themselves. In the first case, the supplies will still exist; the attacker may only have managed to have them shipped to the wrong place or categorized incorrectly. If a cyberspace attacker breaks into the database for a critical warehouse and scrambles it, the parts and equipment are still physically there on the shelves and accessible once the database is rebuilt. Therefore, attacking logistics only through cyberspace will likely not be effective over the long run, it should be integrated into other forms of attack where it can play an important, albeit normally supporting, role. Disruption certainly has its place, and not only in the realm of logistics.

Disrupt Enemy Actions

The fourth way that cyberspace attackers can utilize to connect their cyber means to policy ends is disrupting enemy actions, which may be one of the key contributions of cyberspace attack. Demchak sees disruption as the key element behind all of successful warfare, "Conflict between human societies has always been about successfully disrupting the opponent, whether that opponent was a raiding party, an army, a city, or a whole nation, to get some desired outcome."[41] Demchak overreaches somewhat in claiming that warfare has always been about disruption, but clearly disruption of an enemy can make success much easier. Demchak also thinks that disruption is easier now than it was before as the advent of cyberspace has enabled distant and small-scale opponents to utilize societal disruptions that were previously only available to neighbors

[41] Demchak, *Wars of Disruption and Resilience*, 1.

or superpowers.[42] Here I think she is on firmer ground and it is certainly true that global cyberspace has opened up the possibility of tremendous societal disruption at a distance. However, societal level disruption is not the only thing a cyberspace attacker can aim for.

Attempts to disrupt the enemy's decision-making process are as old as warfare, but cyberspace opens new possibilities, particularly with an enemy that is heavily reliant upon cyberspace systems such as the United States. Even if all an attacker can manage is to introduce some doubt about the veracity of some of the data, it can radically slow decision-making. If a defender discovers that an attacker corrupted a single database, it calls into question if the attacker has also corrupted other databases or systems. [43] According to Libicki, it is not even necessary actually to get into the database and insert false information. An attacker can attack with "noise" or false information fed in from the outside through false reports, intelligence feeds, etc.

> Noise has its place in the arsenal. It can help paralyze or at least inhibit command and control. Under attack, decision makers are not sure that what they know is true, and neither are those who are supposed to carry out their decisions; so, commanders cannot exercise control over their forces or instruments. Even if all a prioris are accurate, the victim's sense that all information flows are fraught with error makes almost every resulting decision tentative. Nothing can be done boldly, cleanly, or decisively. Fall-backs must always be in place.[44]

Disruption through cyberspace attack can produce significant benefits for the attacker, but deliberate misdirection can do even more damage.

---

[42] Demchak, *Wars of Disruption and Resilience*, 2.
[43] Owens, et al., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 113.
[44] Libicki, *Conquest in Cyberspace*, 71.

Misdirect Enemy Actions

The fifth cyberspace way is deception, which can be an even more effective way to utilize cyberspace superiority than disruption. Disruption attacks the enemy's information gathering abilities and attempts to make it difficult for him to communicate and make decisions, while deception attempts to shape the information environment in such a way that the enemy makes decisions favorable to the attacker. An attacker taking down a communications system would be disruption, while the same attacker inserting false information into the system would be deception. Sun Tzu saw deception as the heart of successful warfare and suggested always making efforts to mislead the enemy as to your capabilities and intentions.[45] While Clausewitz did not have as high a view of deception as Sun Tzu did, he saw some use for it and stated that deception was useful as it could encourage the enemy to make mistakes.[46] For an attacker to successfully deceive a defender is actually much harder to do in practice than is commonly understood because it requires understanding the targeted individual's decision-making process at a very deep level.

Deception involves attacking an enemy's mind, and it is most successful when the deception aligns with something the enemy is already inclined to believe. According to Gray, "To deceive, one must first penetrate the cultural veil to comprehend an adversary's world-view so that one can feed his expectations. Since people tend to believe what they want to believe, deception requires an empathy with their adversary's

[45] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith with forward by B. H. Liddell Hart, (London: Oxford University Press, 1971), Kindle Location 1166, chap. 1.
[46] Clausewitz, *On War*, 202.

expectations."[47] The most famous example of this approach is Operation Fortitude where Hitler was convinced that the Allied landing would be at Calais instead of Normandy.[48] Hitler's reluctance to utilize his central reserve because he feared a second landing at Calais gave the Allies critical time to build up their beachhead. More recently, the United States has used deception to great effect in Iraq and against Al-Qaeda.[49] If tying the enemy's decision makers into knots and melting their cyberspace infrastructure does not make the enemy quit, you may have to go and dig him out of his foxhole. Although labeled as mere "support," cyberspace attack can significantly affect the struggle for domain superiority in the other domains.

Support to Other Domain Forces

The final way that cyberspace operators can connect their means with policy ends is through support to the other warfighting domains.[50] Sometimes a combatant will have to fight and defeat the enemy on a physical battlefield. Some analysts such as Libicki believe that cyberspace's greatest contributions will be in support of warfighters in other domains instead of in strategic information warfare.[51] A modern military like that of the U.S. is heavily dependent on cyberspace. For example, consider a small U.S. Army patrol in Afghanistan. On the surface, it might appear that cyberspace forces are not providing anything of importance to the patrol, but as you look deeper, there are numerous cyberspace connections. The patrol likely knows where it is principally

[47] Gray, *Modern Strategy*, 35.
[48] John Keegan, *The Second World War* (New York, Penguin, 1989), 373.
[49] Rosenzweig, *Cyber Warfare*, Kindle Location 1023, chap. 3.
[50] Shawn Brimley, "Promoting Security in Common Domains." *Washington Quarterly* 33, no. 3 (2010): 122.
[51] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), 6.

through space based GPS, which is highly dependent upon cyberspace for command and control. The military has also linked those GPS systems into a "blue force tracking" system that provides information to headquarters on the location of the patrol, and information on other friendly forces to the patrol. A logistical system completely dependent upon cyberspace brought the vehicles the patrol is riding in, as well as the people, their weapons, ammunition, and food into country. An Air Tasking Order (ATO) built and disseminated in cyberspace put the fighter aircraft overhead providing top cover and the weapons on board the aircraft were mission planned on a network of computers vulnerable to cyberspace attack. Digging further reveals more and more links to cyberspace for modern military forces, but there are some limitations in attacking those links.

Offensive cyberspace support to other domain forces has some limitations due to the difficulty in receiving accurate and timely assessment of its effects. It will often be unclear if the attacker has really disrupted the enemy system or if the enemy is merely making it look like the attacker was successful. Consider an attacker that disables an enemy IADS to allow an airborne strike package to hit its targets. The cyberspace operators can verify that they sent the command to shut down the IADS and the radars have all gone offline, but is that because the attack was successful or because the enemy is waiting to ambush the strike package? Because of this uncertainty, warfighters will often still prefer to put a bomb on the radar, as physical destruction is more certain. Libicki has identified that while using offensive cyberspace operations in support of an attack may be prudent, betting the entire operation on the success of that cyberspace

attack may not be.[52] Cyberspace defenders are not going to sit idly by while attackers connect their cyberspace ways and means; instead, they are going to try actively to block them.

Cyberspace Defensive Blocks

Cyberspace attackers do not have such an overwhelming advantage that cyberspace defenders cannot effectively contest cyberspace superiority. While machines are brittle and do not react well to change or conditions that they do not expect, cyberspace is a domain in which people operate, not just machines. Humans excel at adapting and responding to changes in their environment. Some authors have put so much emphasis on offensive cyberspace capabilities that they have been dismissive of the capabilities of cyberspace defense. This situation parallels the early days of airpower when Stanley Baldwin overstated the power of the offensive in the air and famously stated that, "the bomber will always get through."[53] Stanley Baldwin was wrong, and so are his equivalents in the cyberspace domain today. There are some potential changes in cyberspace that may favor the defender.

Several developments could swing the advantage in cyberspace towards the defense. One development is that engineers are working on new protocols that might make some of the issues with attribution less difficult. It is possible that some of these ideas will result in separate "trusted" Internets that are easier to defend, as actors have to give up anonymity to enter. Other defensive technologies such as firewalls and intrusion

[52] Libicki, *Cyberdeterrence and Cyberwar*, xv.
[53] Stanley Baldwin, "A Fear for the Future," Speech given in Parliament 10 November 1932. http://en.wikisource.org/wiki/A_Fear_For_The_Future.

systems continue to improve and there are policy changes that Congress could implement that would significantly change the playing field as well. Right now, most attacks come through zombies and botnets. Often Internet Service Providers (ISPs) or security agencies can readily identify these machines, but they cannot do anything about them under current law, since private third parties own them. If cyberspace attacks became more disruptive, Congress could change the law to enable authorities to remove these computers from the Internet until their owners had cleaned them. There are also other policy changes that politicians could make, for example, to require industry to meet some minimum standards for the defense of their networks. Right now, there is not sufficient political will to implement these policy changes. However, it is not hard to imagine how a major cyberspace attack could dramatically change that environment.

Cyberspace defenders are not completely without tools even today that they can use to sever the connection between an attacker's means and ways to gain cyberspace superiority. Defenders stop the vast majority of cyberspace attacks now with simple defenses. After examining cyberspace offense and defense, Libicki concluded that, "in this medium, the best defense is not necessarily a good offense; it is usually a good defense."[54] In the rest of this section, I will lay out a number of the tools currently available to cyberspace defenders.

Firewalls, Intrusion Detection Systems, and Closing Vulnerabilities

The first block a defender can rely on to contest cyberspace superiority consist of firewalls, intrusion detection systems (IDS), and closing vulnerabilities. Firewalls

[54] Libicki, *Cyberdeterrence and Cyberwar*, 176.

operate by attempting to separate out legitimate Internet traffic from illegitimate. They can be either hardware or software related and sit at a communications node where they examine each network packet and determine whether to send it onto its destination based on a set of rules. For example, a firewall would likely allow an outbound connection from a user to connect to www.microsoft.com, and then would let the information sent back from www.microsoft.com through the port. On the other hand, a firewall would block an unsolicited packet from the IP address associated with www.evilhackersrus.net. The rule set is of course far more complex and involves monitoring the types of packets, which programs are accessing which ports and many other pieces of information. Firewalls are a networks first line of defense and can screen out a large number of low-level unsophisticated attacks. Hackers will compromise a clean computer with no firewall connected to the Internet in minutes. From January to July of 2013, researchers found that the average "survival time" was less than two minutes.[55] A firewall is only one component of a basic defense; the second is an intrusion detection system.

A firewall is like a lock that attempts to keep the burglar out, while an IDS is the alarm that goes off if he successfully breaks in. According to the System Administration, Networking, and Security institute (SANS), an intrusion detection system "is a security system that monitors computer systems and network traffic and analyzes that traffic for possible hostile attacks originating from outside the organization and also for system

[55] SANS Technology Institute, "Survival Time," *Internet Storm Center*, Graph generated from 1 Jan 2013 to 30 July 2013 on 31 August 2013. http://isc.sans.edu/survivaltime.html.

misuse or attacks originating from inside the organization."[56] An IDS can be a simple consumer package that operates automatically, or it can be a monitored system with human interface and intervention. The firewall and IDS on a network are the first line of defense, but almost as important is trying to limit what damage a malicious actor can do when he gets in by reducing vulnerabilities.

Just getting into a network is only the first step for a cyberspace attacker. Once he burrows through the walls, he is normally going to need a vulnerability to exploit. Unfortunately, system administrators often do not keep their systems fully patched. According to a 2013 survey, 17% of security professionals admitted that they have not fully patched the enterprise operating systems under their care.[57] The CERT coordination center estimates that keeping up to date with appropriate patches could avoid 95% of all network intrusions across enterprise and private computers.[58] Closing known vulnerabilities is the minimum bar for cyberspace defenders; they can go further and aggressively seek out unknown vulnerabilities. It is also critical for system administrators to disable unused services, as that will close off entire sections of potential vulnerabilities. Owens and Dam have noted that an unneeded capability brings unnecessary additional vulnerability, so every "nice-to-have" feature increases risk for

[56] SANS, "Intrusion Detection Systems: Definition, Need and Challenges," *SANS*, 2001. http://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-systems-definition-challenges-343.
[57] Kelly Jackson Higgins, "Nearly One-Fifth of Enterprise Operating Systems not Fully Patched," *Security Dark Reading*, 23 August 2013. http://www.darkreading.com/vulnerability/nearly-one-fifth-of-enterprise-operating/240160403.
[58] USDA, "Patch Management and Systems Updates," Accessed 31 August 2013. http://www.ocio.usda.gov/sites/default/files/docs/2012/DM3535-002.htm.

the entire system.[59] Firewalls, IDS, and patching software vulnerabilities are the first line of defense, but defenders must also attack the weaknesses of the human element of the system as well.

Hardening Users via Training

The second block that a cyberspace defender can utilize to contest cyberspace superiority is to increase the capability of the humans using the system. Users are the bane of system administrators the world over and many attacks rely on finding a user who can be tricked into doing something to compromise the system. Most users have only a rudimentary knowledge of computer security, so spending time and money training them can produce a significant payoff. Mandatory training programs are a start, but not all users will pay attention to training or be convinced that it is important to them. System administrators need to convince the users that there is significant benefit to following good security practices whether it is monetary rewards for best practices or reprimands for those who do not follow procedures. An active and aggressive "red team" program is essential to have, not just for the network, but also to have the users probed on a regular basis to see where security practices are weak and whom an attacker can trick into providing access. Performance ratings and rewards need to be explicitly tied to following security practices and those who cannot follow proper protocols may need to be fired to emphasize that the organization is taking security seriously.

Without aggressive action to provide training, and incentivize good security practices, organizations will still remain vulnerable to social engineering, which is one of

[59] Owens, et al., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 84.

the most common ways that a cyberspace attacker can utilize to connect their means and ways. As an example, in a recent study, security testers left USB thumb drives on the ground in a parking lot outside of a federal office building. All federal employees receive regular training on the dangers of plugging in unknown USB devices, but 60% of these highly trained employees plugged them in anyway. The addition of an official looking logo on the drive increased the percentage of USB drives employees plugged in to 90%.[60] Clearly simple training is not enough, so system administrators are also turning to increasing restrictions and controls on users.

Increasing Restriction and Controls on Users

A third way for a defender to block a cyberspace attacker from achieving cyberspace superiority is through increasing restriction and controls on users. According to Libicki, "It is only a modest exaggeration to say that organizations are vulnerable to cyberattack only to the extent they want to be. In no other domain of warfare can such a statement be made."[61] At the extreme end, network administrators could disconnect every wire in the network and power off every device. The network would be "safe" but also useless. The purpose of information systems is to process and share information; if overzealous system administrators can be convinced to shut systems off from the outside world that may actually hand the attacker cyberspace superiority. A cyberspace defender who shuts down and "protects" his system is doing the same thing the Iraqi Air Force did in the air domain by flying their aircraft to Iran during the Gulf War. The assets were "protected," but also completely useless in the conflict at hand. It is critical to find the

[60] Rosenzweig, *Cyber Warfare*, Kindle Location 815, chap. 3.
[61] Libicki, *Cyberdeterrence and Cyberwar*, xiv.

right balance between access and security so that defenders can avoid doing the attacker's work for him. Marjory Blumenthal and David Clark have identified that as, "…the key paradox of securing the Internet: it is the act of communication that is risky, but communication is the whole goal of the Internet."[62] In situations where security is more critical than communication, cyberspace defenders can turn to the next block of "air gapping" their systems.

Air Gap Critical Systems

A fourth way that a defender can attempt to deny an attacker cyberspace superiority is through air gapping. Air gapping refers to disconnecting a system from the rest of the Internet. Early on, most SCADA systems were air gapped and they performed their control tasks without any access or communication to the outside world. Often classified systems are air gapped and built as a separate stand-alone network. It is not always the case that air gapped systems are physically air gapped. It is also possible to separate a system from the Internet by encrypting it. A combatant might still use major transoceanic cables to move the data, but encrypt the data to prevent attackers from accessing the network information. Just as there are multiple ways of setting up an air gap, there are also many ways to cross it for an attacker, so it is not an absolute defense. An attacker can use physical media such as USB flash drives or CDs inserted by spies or unwitting accessories such as the federal employees discussed earlier. There is also the avenue of wireless network attack, which was discussed in the cyberspace means section

[62] Marjory S. Blumenthal and David D. Clark, "The Future of the Internet and Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, DC: Potomac Books, 2009), 229.

earlier. It only takes one computer on the network that an administrator forgot to disable the wireless modem to give an attacker a back door into the entire network. Finally, if an attacker can physically access the cables carrying an air-gapped system, it could disrupt the network by interfering with the traffic even if the encryption could not be broken.

Cryptography, Passwords, and Biometrics

The fifth defensive block that defenders can use to stop attackers from gaining cyberspace superiority is by utilizing cryptography, passwords, and biometrics. Cryptography makes it more difficult for attackers to access information and manipulate cyberspace systems. Passwords are a basic defense much like firewalls or an IDS, and there are few significant systems that do not require a password for access. However, passwords can often be broken rather easily if users do not build strong ones, but strong passwords are hard to remember and users will often choose weaker passwords. Hackers can easily break weaker passwords by utilizing dictionaries of commonly used passwords. Believe it or not, the most common password in the world is still "password."[63] In the constant war between system administrators and users, the system administrators set up more difficult password rules and the users figure out ways to circumvent them to generate passwords they can actually remember. No one can remember 27 different random 15-character passwords without either writing them down, or utilizing the same one or variations, but fortunately, there are other solutions.

One way out of the dilemma of secure passwords being too difficult to remember is to use a physical token such as a Department of Defense Common Access Card (CAC)

[63] Chenda Ngak, "The 25 most common passwords of 2012," *CBS News*, 24 October 2012. http://www.cbsnews.com/8301-205_162-57539366/the-25-most-common-passwords-of-2012/.

coupled with a single password. This token system makes it more difficult for a hacker and easier for the user as long as they physically have the card. Another approach is to utilize biometrics where the user him or herself is the physical token. In the past, cyberspace defenders have used fingerprint and retina scans as biometric access control measures. These techniques are not unbreakable if a defender does not implement them properly. A defender can leave holes by not implementing biometrics correctly, but they can also be a step forward. Every technique is going to have some weakness and defenders do well to plan for failure and have a plan to quickly recover and reconstitute.

Increasing Resilience

The sixth way that a defender can use to deny an attacker cyberspace superiority is through increasing resilience. Even if a defender cannot completely stop an attacker, a quick recovery can diminish the cyberspace superiority achieved by the attacker. Historically, cyberspace resilience has been fairly robust. Despite the media attention given to major worms such as Melissa or Slammer, most IT operations were back in full operation in a couple of days.[64] A cyberspace defender should plan their system to be resilient. Resiliency is both withstanding shocks, and being able to recover from misfortune.[65] Both aspects apply to the type of resilience needed by defenders, as systems must to be able to absorb attacks and continue to function as well as recover quickly if attackers disrupt them. According to Rosenzweig, systems need to be, "robust,

[64] Libicki, *Conquest in Cyberspace*, 37.
[65] Merriam-Webster Dictionary, "Resilient, adj," Merriam-Webster, Incorporated. http://www.merriam-webster.com/dictionary/resilient

adaptable, and capable of rapid response and recovery."[66] A critical element of this resilience is that defenders can make copies of the data and programs on their systems.

Backups enable a defender to rapidly reconstitute damaged systems and data, and therefore limit the amount of cyberspace superiority an attacker can achieve. An attacker who breaks into a logistics system and erases all the data can cause significant problems for a defender. If the defender has a backup and can have the system restored and operating in a day, the defender can minimize the attack's long-term effects. One of the hopeful trends for cyberspace defenders is the decreasing cost of electronic data storage. This decreasing cost makes it far easier for defenders to keep one, two, or ten copies of the data needed to restore a system. Of course, defenders need to keep the copies in a manner that prevents an attacker from getting to the backups and the primary system at the same time. Automatic backup systems may be convenient, but they are automatic and will copy a cyberspace weapon just as easily as valid data. Backups are part of resilience, but defenders should also structure their systems to maximize resilience.

Cyberspace defenders should not assume success when designing their systems, but instead should plan for failure. Rosenzweig has identified that there are other systems, such as the electric grid, where designers plan for failure and build in significant resiliency and redundancy.[67] As much as possible, defenders need to build networks so that the disruption of a single node does not prevent the entire system from functioning. There is promise in cloud computing although there are some new dangers as well. Cyberspace defenders need to practice against large-scale disruptions, which is hard to do

[66] Rosenzweig, *Cyber Warfare*, Kindle Location 3775, chap. 17.
[67] Rosenzweig, *Cyber Warfare*, Kindle Location 3727, chap. 16.

without being in a cyberspace training range. The local base commander will likely not want his or her network to go down for a week so that the cyberspace warriors can build it up again. This tension between training and operations is only one of the cultural tensions engendered by a resiliency-focused defense.

Shifting to a resiliency-focused defense involves a paradigm shift that is difficult for many military officers. Antoine Bousquet has highlighted the U.S. military's tendency to strive for "100% relevant content, 100% accuracy, and zero time delay" to allow, "the perfect operation of a frictionless cybernetic war machine."[68] Resilience instead calls for embracing uncertainty and designing for failure and the unforeseen. The supposed revolution in military affairs that was going to dissipate the Clausewitzian "fog" through perfect information has largely been discredited, but it still echoes in U.S. military cultural preferences to pursue perfect information. It is not just the cyberspace warriors who need to adapt, operators and support personnel who focus on the other domains also need to practice operating effectively in an environment where not everything works. Although this training is easiest for defenders to accomplish in difficult exercise scenarios, the defenders in the United States military do not often practice against difficult scenarios due to a cultural fear of failure. When is the last time a U.S. military unit fought an exercise "war" with none of their computers working? It is possible, previous generations did it for years before the construction of computers, but without practicing it, the capability will not be there when needed. Combatants need to prepare for failure and be able to continue fighting, even if they temporarily lose

[68] Antoine Bousquet, *The Scientific Way of Warfare* (New York: Columbia University Press, 2009), 156.

cyberspace superiority in certain systems. One way to mitigate some attacks is to divert them somewhere that they will not do any damage.

Honey Nets

The seventh defensive block that a defender can utilize to keep an attacker from attaining cyberspace superiority is a honey net. A honey net diverts attackers into a false network full of whatever the defender wants the attacker to see. If a cyberspace attacker is attempting to break into a highly classified compound and the defenders know it, they can divert him into a false network. If you block the attacker, there is nothing preventing him from trying again using a different access that the defender might miss. If the defender instead diverts the attacker but provides him with false information, that can be far more effective. Something similar to this happened in the early 1980s when a U.S. spy provided information that the Soviet Union was planning secretly to acquire gas pipeline technology. Instead of blocking the sale, the U.S. quietly altered the computer code that eventually led to, "the most monumental non-nuclear explosion and fire ever seen from space."[69] Defenders can do much the same thing in cyberspace. Once a defender captures an attacker in a honey net, the defender can keep the attacker busy with false information, examine attack patterns and techniques, or whatever is most useful. One of the most useful techniques for a defender is instilling doubt in the mind of the attacker.

Introducing doubt into the mind of an attacker through a honey net can affect the attacker's connection of cyberspace means and ways in other cyberspace attacks as well.

[69] O'Harrow, *Zero Day*, Kindle Location 345, part 2.

A defender does not have to falsify everything; successfully falsifying one piece of information can make the attacker doubt everything else he got as well. One way of accomplishing this increased doubt is through a defender falsifying Battle Damage Assessment (BDA.) It is normally difficult for an attacker to understand how effective his attacks have been; a honey net can make it even worse. A defender can use a honey net to make it look like an attack has been successful, but then suddenly turn the system back on to ambush the attacker's forces at the most opportune time.[70] Tricking the enemy this way once, will also have the tendency of making the enemy very reluctant to trust any future cyberspace BDA. This potential for false BDA is why airmen are generally not very enthusiastic when a cyberspace warrior tells them he or she is "pretty sure" the SAM system they are going to fly over has been disabled. The tendency of warfighters is to put a bomb on it anyway, just in case, which diminishes the utility of the cyberspace attack. Honey nets are powerful tools for defenders in cyberspace, but there are some even more powerful techniques taken from the attackers themselves.

Active Defenses and Hackbacks

The final way that a defender can contest cyberspace superiority is through active defense and hackbacks. According to Clausewitz, defenders should not simply wait passively, "…the defensive form of war is not a simple shield, but a shield made up of well-directed blows."[71] Active defenses and hackbacks are a critical part of the defender's arsenal, and if they are not used, significantly constrain the defender's

[70] Owens, et al., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 125.
[71] Clausewitz, *On War*, 357.

effectiveness. Owens, Dam, and Lin identified that with only a passive defense the defenders have to succeed every time, and since there are no penalties for the attacker, he can continue attacking until he is successful.[72] This difference places, "a heavy and asymmetric burden on a defensive posture that employs only passive defense."[73] A defender can be attempting to accomplish several things when utilizing active defenses. A defender can disable the computers executing the attack. A defender can also attempt to trace an attack back to its source. Attackers will normally bounce attacks through multiple servers to attempt to hide themselves, but a persistent defender can sometimes work back through the servers to the source. If a defender makes it all the way back to the originator of the attack, there are now a number of unpleasant things he or she could theoretically do to the attacker's networks in retaliation. Unfortunately, most of those things are currently illegal for defenders to do under U.S. law.

Since active defense normally involves breaking into a number of privately owned computers along the way, it is generally illegal under the Computer Fraud and Abuse Act (CFAA.) According to Rosenzweig, any active defense that reaches outside of the defender's computer system is "almost certainly a crime in and of itself."[74] This legal issue opens cyberspace defenders up to prosecution and lawsuits whether they are military or civilian. And that is just if the attacking computers are only in the United States, which is normally not going to be the case. Breaking into computers in foreign countries brings on an entirely new set of legal and political problems. The difficulty in

[72] Owens, et al., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 13.
[73] Owens, et al., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 13.
[74] Rosenzweig, *Cyber Warfare*, Kindle Location 2024, chap. 7.

attributing attacks might work in the defender's favor, as it can be hard to attribute hackbacks if the defender chooses to use the same techniques to mask where he is coming from, but that does not deal with the legal and ethical issues. Hackbacks quickly devolve into a legal and political Gordian knot. Active defenses are required for effective defense, but they are clearly illegal, and just as clearly even private organizations are now using them.[75] Hopefully, policy and legal authorities will catch up in this important area. Attackers are just as capable of reacting as defenders, and have some tools and techniques they can use to overcome these defensive blocks.

Counters to Defensive Blocks

Cyberspace forces can and do "maneuver" against each other in cyberspace. Some analysts have been too deterministic and have argued that cyberspace weapons do not have the capability to maneuver. As I noted earlier, cyberspace is a blending of brittle technology and flexible people. The technology may not be able to maneuver, but the people can and will. We just finished examining defensive blocks, the attacker gets to react as well and "maneuver" in response.

Utilize Training to Refine Social Engineering

The first way that an attacker can attempt to degrade defensive cyberspace blocks preventing him from achieving cyberspace superiority is through refinement of social engineering based on the defender's own training program. If there is a means of social networking that the defender has not covered in the training that may be a good avenue of attack to pursue. Another possibility would be for an attacker to look at any examples

[75] Kelly Jackson Higgins, "Free 'Active Defense' Tools Emerge," *Security Dark Reading*, 11 July 2013. http://www.darkreading.com/intrusion-prevention/free-active-defense-tools-emerge/240158160.

given in training as to what is acceptable and what is not, and then design attacks that look like the acceptable examples as much as possible but actually compromise the system. Depending on the quality of the training, there may be significant mistakes or old information that an attacker can exploit. Even if the training is extremely thorough, knowing how a defender trained employees can provide insights useful to the attacker. "Dumpster diving" for unclassified, but useful information can provide a gold mine of information that can also allow attackers to focus their social engineering attacks. If social engineering is not providing access, an attacker can always switch to machine versus human based attacks through code and password cracking.

Code and Password Cracking

A second method attackers can utilize to overcome defensive blocks is code and password cracking. As noted in the defensive block section, properly encrypted information should be almost impossible to break with current technology, however the same was true of the German Enigma machine in World War II and it was broken anyway.[76] The Allies broke the German codes through a suite of techniques that mostly relied on human errors in implementing the code system, not in breaking the system itself via "brute force" methods. Humans are no less likely to make mistakes in procedures today than they were in the 1940s and so there are still many opportunities for code-breakers to exploit, even if the codes themselves are "impossible" to break. Any code can be broken if a "trusted agent" is actually passing information to the other side, and

[76] R. A. Ratcliff, *Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers* (Cambridge: Cambridge University Press, 2006), 2.

sometimes a single weak password can be used by an attacker to leverage access to other passwords and systems.

If an attacker cannot trick someone into giving up their password via social engineering, a weak password may fall to brute force password cracking methods. In addition, an individual may use the same password on more than one system and if an attacker can break into a less secured system, he may now have the keys to the more secure system. Understanding the training that users get can also help refine attacks on passwords. If the defender trained users to utilize geometric patterns to generate passwords, then those can be included in the attacker's password dictionary. In cryptography, persistence is often the key to success as it is in some other types of cyberspace attacks.

Simultaneous and Persistent Attacks

A third way for attackers to outmaneuver defenders and gain cyberspace superiority is through simultaneous and persistent attacks. Persistence is an important avenue of attack to overcome various defensive blocks, not just in cryptography. Libicki highlights the difficulty of permanently damaging systems through cyberspace and notes that system administrators can generally restore network performance within 48 hours while preventing further attacks using the same weapon.[77] Accordingly, for an attacker to be persistent will normally require a timed cascade of different attacks instead of sending more of the same attack. Owens, Dam and Lin highlight that it is actually easier for an attacker to be successful in the first attack versus follow up attacks because the

[77] Libicki, *Conquest in Cyberspace*, 37.

defenders learn from the attack and close down access avenues.[78] The requirement for persistence is not unique to the cyberspace domain, air planners know that just because an enemy airfield has been "destroyed" it does not mean it is going to stay destroyed. There are several elements of persistence in the cyberspace domain that attackers should consider.

It is important to note two caveats to persistence by an attacker. First, doubling of effort does not necessarily correspond to doubling of effect. From Libicki, "Alas, it is too easy to react to insufficient BDA information by attacking repeatedly, but doubling the effort may reduce the effect."[79] Secondly, a cyberspace attacker does not need mulish persistency. Persistence must be flexible, creative and not simply be more of the same attack. This need for flexibility is true of the other physical domains as well and Luttwak captures this concept when he states that, "Sheer persistence is the key to success in all things, except in war, when only those who persist flexibly can hope to prevail."[80] One way for an attacker to introduce flexibility is not to metaphorically charge straight up the same hill; instead an attacker should charge the hill from multiple directions.

Simultaneous attack is a critical tool in the cyberspace attacker's toolkit to mitigate defensive blocks. Distributed Denial of Service (DDoS) attacks rely on this simultaneity as a defender can shrug off an attack from a single computer easily. A 10,000-computer botnet is much harder to ignore as the attacks come from all directions. It is also important that an attacker attempt to build as many points of access as possible

[78] Owens, et al., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 112-113.
[79] Libicki, *Conquest in Cyberspace*, 87.
[80] Luttwak, *Strategy: The Logic of War and Peace*, 200.

so that if the defender finds and seals one access point the attacks can still continue. Another form of simultaneous attack is to go after more than one component of a system. For example, instead of just attacking on the software side, there are ways to attack hardware as well.

Attacking both the hardware and software components of a system is a way for attackers to utilize simultaneous attack to seek cyberspace superiority. Although the regular Internet hoaxes about viruses that have the ability to melt your computer into a puddle of goo overstate the threat, it is possible to damage hardware via techniques such as shutting down cooling systems and deliberately causing hardware to overheat. Damaged hardware can greatly increase the persistence of attacks, as it takes much longer for a defender to recover functionality. It is also important for a cyberspace attacker to go after backup systems at the same time whenever possible to prevent easy recovery by the defender. Simultaneous attacks will also often be required when an attacker is attempting to breach a highly secured system protected by an air gap.

Non-Internet Based Attacks

The final method that cyberspace attackers can utilize to evade defensive blocks is Non-Internet based attacks. These attacks are particularly important in accessing air-gapped systems. Air gapped systems are difficult, but not impossible to access and often the access point will be provided through mistakes made by humans operating the system. A wireless modem that was inadvertently left or turned on, a hardware or software based attack through inserting malicious code in the defender's supply chain, and physical access to the system through espionage or special operations are all possibilities. There are air gaps that attackers have successfully crossed in the past;

Stuxnet is the best-known example where a cyberspace weapon penetrated into a highly secured nuclear site in Iran. One of the problems with keeping security on an air-gapped system is that engineers need to maintain and update it. To accomplish updates, they normally do not rewrite code on the air gapped computer terminal, but insert updates from another machine that an engineer has temporarily connected to the secured system. However, if an attacker has secretly compromised the maintenance computer, it presents an opportunity for a weapon to access the secured system every time a computer or storage device is connected.

Attackers and defenders will continue to develop other tools and techniques over time, but the ones presented here provide an overview of what is currently possible in the rapidly changing cyberspace domain.

BIBLIOGRAPHY

Adee, Sally. "The Hunt for the Kill Switch." *IEEE Spectrum*, 2008. http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0.

Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations,* Change 1. 30 November 2011.

Alberts, David S., John J. Garstka, Richard E. Hayes, and David A. Signori. *Understanding Information Age Warfare.* CCRP publication series. Washington, DC: DOD, 2001.

Arias, Jorge and Guilherme Venere. "South Korean Banks, Media Companies Targeted by Destructive Malware." *McAfee Blog Central*, 20 March 2013. http://blogs.mcafee.com/mcafee-labs/south-korean-banks-media-companies-targeted-by-destructive-malware.

Associated Press. "Debate over possible responses to cyber attacks: Analysts say punishment needs to fit crime, but was assault an act of war?" *NBC News*, 9 July 2009. http://www.nbcnews.com/id/31836856/ns/technology_and_science-security/.

Associated Press. "Official: North Korea believed behind cyber attacks." *Jakarta Post,* 8 July 2009. http://www.thejakartapost.com/news/2009/07/08/official-north-korea-believed-behind-cyber-attacks.html.

Associated Press. "N. Korea denies hacking into SKorean bank's network." *Jakarta Post,* 10 May 2011. http://www.thejakartapost.com/news/2011/05/10/n-korea-denies-hacking-skorean-banks-network.html.

Associated Press. "N. Korea Suspected of Global Cyber Attack." *NBC News*, 8 July 2009. http://www.cbsnews.com/stories/2009/07/08/tech/main5143457.shtml.

Associated Press. "North Korean army suspected in cyber attacks: Hackers told to 'destroy' South Korean communications, report says." *NBC News*, 11 July 2009. http://www.nbcnews.com/id/31866018/ns/world_news-asiapacific/.

Associated Press. "US officials eye North Korea in cyber attack." *Jakarta Post*, 9 July 2009. http://www.thejakartapost.com/news/2009/07/09/us-officials-eye-north-korea-cyber-attack.html.

Baker, Meredith Attwell. "Hands Off Tomorrow's Internet." *The Washington Post*, 21 December 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/12/20/AR2010122003901.html.

Baldor, Lolita. "Government-backed Hacker Teams do Most China-based Data Theft." *USA Today,* 12 December 2011. http://www.usatoday.com/tech/news/story/2011-12-12/chinese-hackers/51830840/1.

Baldor, Lolita. "US officials eye North Korea in cyber attack." *Tulsa World,* 8 July 2009. http://www.tulsaworld.com/article.aspx/US_officials_eye_North_Korea_in_cyber_attack/20090708_13_0_seouls64065.

Baldor, Lolita. "White House among targets of cyber attack: Other targets included NSA, Homeland Security and State Department." *NBC News*, 8 July 2009. http://www.nbcnews.com/id/31800532/ns/technology_and_science-security/.

Baldor, Lolita and Jordan Robertson. "Experts work to untangle US, Korea cyber attack." *Omaha World-Herald*, 9 July 2009. http://www.omaha.com/article/20090708/AP13/307089964.

Baldwin, Clare and Jim Christie. "Cyber attacks may not have come from North Korea." *Reuters*, 8 July 2009. http://www.reuters.com/article/2009/07/09/us-internet-security-analysis-idUSTRE5680C220090709.

Ballenstedt, Brittany. "Expert Flags Flaw in Cyber Workforce Plan." In Wired Workplace, edited by nextgov, Web blog regarding cyber issues at the government level, 2011, http://www.nextgov.com/cio-briefing/wired-workplace/2011/08/expert-flags-flaw-in-cyber-workforce-plan/54777/.

Barnes, Ed. "North Korea's Cyber Army Gets Increasingly Sophisticated." *Fox News*, 17 May 2011. http://www.foxnews.com/world/2011/05/17/north-koreas-cyber-army-gets-increasingly-sophisticated/.

Barrett, Major General Mark, Dick Bedford, Elizabeth Skinner, and Eva Vergles. "Assured Access to the Global Commons." Edited by Supreme Allied Command Transformation. Norfolk, VA: North Atlantic Treaty Organization, 2011.

Belk, Robert and Matthew Noyes. "On the Use of Offensive Cyber Capabilities." Master's Thesis, Harvard Kennedy School, 2012.

Bloch, Marc. *The Historian's Craft.* Translated by Peter Putnam. New York: Alfred A. Knopf, 1953.

Blumenthal, Marjory S., and David D. Clark. "The Future of the Internet and Cyberpower." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 206-240. Washington, DC: Potomac Books, 2009.

Bousquet, Antoine. *The Scientific Way of Warfare.* New York: Columbia University Press, 2009.

Brimley, Shawn. "Promoting Security in Common Domains." *Washington Quarterly* 33, no. 3 (2010): 119-32.

British Broadcasting Corporation. "North Korea 'behind South Korean bank cyber hack'." *BBC*, 3 May 2011. http://www.bbc.co.uk/news/world-asia-pacific-13263888.

British Broadcasting Corporation. "Russia in Georgia separatist pact." *BBC*, 17 September 2008. http://news.bbc.co.uk/2/hi/europe/7620972.stm.

Brito, Jerry, and Tate Watkins. "The Cybersecurity-Industrial Complex: The Feds Erect a Bureaucracy to Combat a Questionable Threat." *Reason 43*, no. 4 (2011): 7.

Bronk, Christopher and Eneken Tikk-Ringas. "Hack or Attack? Shamoon and the Evolution of Cyber Conflict." James A Baker III Institute for Public Policy Working Paper, 1 February 2013.

Bryant, William D. "Cyberspace Superiority: A Conceptual Model." *Air Space Power Journal*, Volume 28, no. 3 (2014): 25-44.

Bush Administration. "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection." Edited by Executive Office of the President, Washington, DC, 2003.

Butler, Sean C. "Refocusing Cyber Warfare Thought." *Air Space Power Journal*, Volume 27, no. 1 (2013): 44-57.

Cable News Network. "A convicted hacker debunks some myths." *Cable News Network*, 13 October 2005. http://www.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/.

Cable News Network. "Russia-Georgia tensions still high one year on from conflict." *Cable News Network*, 7 August 2009. http://www.cnn.com/2009/WORLD/europe/08/07/goergia.background/.

Cahanin, Steven E. "Principles of War for Cyberspace." Air War College, 2011.

Carter, Jerry and Fred Taylor. "Cyberspace Superiority: An analysis of the Department of Defense's Ability to Achieve Superiority in Cyberspace." Master's Thesis, Harvard John F. Kennedy School of Government, 2011.

Cartwright, James E. General, USMC. "AFA's 2007 Air Warfare Symposium Transcripts." Air Force Association, 2007. http://www.afa.org/events/AWS/2007/post_Orlando/scripts/cartwright.asp.

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld.* Beijing: O'Reilly Media, 2011. Kindle edition.

Carr, Jeffrey. "Who's Responsible for the Saudi Aramco Network Attack?" *Infosec Island*, 28 August 2012. http://www.infosecisland.com/blogview/22290-Whos-Responsible-for-the-Saudi-Aramco-Network-Attack.html.

Chosunilbo. "Cyber Security Is Vital for National Defense." *The Chosunilbo*, 23 August 2013. http://english.chosun.com/site/data/html_dir/2009/11/02/2009110200788.html.

Chosunilbo. "Reports: New Evidence Points to N. Korean in Cyber Attacks." *The Chosunilbo*, 22 August 2013. http://english.chosun.com/site/data/html_dir/2009/07/12/2009071200931.html.

Claburn, Thomas. "Cyber Attack Against Georgia Blurred Civilian and Military." *Information Week*, 17 August 2009. http://www.informationweek.com/government/security/cyber-attack-against-georgia-blurred-civ/219400248.

Clancy, James and Chuck Crossett. "Measuring Effectiveness in Irregular Warfare." *Parameters*, Summer 2007, 88-100.

Clark, Colin. "US Blew NK Cyber Attacks." *DoD Buzz*, 13 July 2009. http://www.dodbuzz.com/2009/07/13/7833/.

Clark, David. "Characterizing cyberspace: past, present and future." MIT CSAIL, Version 1.2. 12 March 2010.

Clark, David. "Three Views of Cyberspace." Version 3.1. 5 January 2011.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat To National Security And What To Do About It.* 1st ed. New York, NY: ECCO, 2010.

Clarke, Richard. "China's Cyberassault on America." *The Wall Street Journal*, 2011. http://online.wsj.com/article/SB10001424052702304259304576373391101828876.html?mod=wsj_share_facebook.

Clarke, Richard. "Software Power: Cyber Warfare is the Risky New Frontline." Harvard Kennedy School. http://www.powerandpolicy.com/2011/02/07/software-power-cyber-warfare-is-the-risky-new-frontline/.

Clausewitz, Carl von. *On War.* Edited and Translated by Peter Paret and Michael Howard. Princeton, NJ: Princeton University Press, 1976.

Cohen, Ariel and Robert E. Hamilton. *The Russian Military and the Georgia War: Lessons and Implications.* Carlisle, PA: Strategic Studies Institute, 2011.

Corbett, Sir Julian Stafford. *Some Principles of Maritime Strategy, Classics of Sea Power*. Annapolis, MD: Naval Institute Press, 1988.

Corbin, Kenneth. "Lessons From the Russia-Georgia Cyberwar." *Internet News*, 12 March 2009. http://www.internetnews.com/government/article.php/3810011/Lessons-From-the-Russia-Georgia-Cyberwar.htm.

Convertino, Sebastian, M. Lou Anne DeMattei, and Tammy M. Knierim. "Flying and Fighting in Cyberspace," Maxwell Air Force Base: Air University, 2007.

Crosston, Matthew D. "World Gone Cyber MAD: How 'Mutually Assured Debilitation' Is the Best Hope for Cyber Deterrence." *Strategic Studies Quarterly*, Volume 5, no. 1 (Spring 2011): 100-116.

Danchev, Dancho. "Study finds the average price for renting a botnet." *ZDNet*, 26 May 2010. http://www.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528.

De Seversky, Alexander P. *Victory Through Air Power*. New York, NY: Simon and Schuster, 1942.

De Seversky, Alexander P. *Air Power: Key to Survival*. New York, NY: Simon and Schuster, 1950.

"Defending the Networks: The NATO Policy on Cyber Defence." edited by NATO Public Diplomacy Division. Brussels, BE: North AtlanticTreaty Organization, 2011.

Demchak, Chris C. *Wars of Disruption and Resilience.* Athens: The University of Georgia Press, 2011.

Demchak, Chris C. and Peter Dombrowski. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly*, Spring 2011: 32-61.

Denmark, Abraham M., and James Mulvenon, eds. "Contested Commons: The Future of American Power in a Multipolar World." Center for a New American Security, 2010.

Department of Defense, *Joint Publication 1-02*, 15 December 2012.

Dictionary, Merriam-Webster. "Superior, adj." Merriam-Webster, Incorporated, http://www.merriam-webster.com/dictionary/superior?show=0&t=1376346445.

Douhet, Giulio. *The Command of the Air*. Mechanicsburg, PA: Stackpole Books 1921. Reprint, 1999.

Dunlap, Charles Jr., Major General, USAF Retired. "Perspectives for Cyber Strategists on Law for Cyberwar." *Strategic Studies Quarterly* 5, no. 1 (2011): 81-99.

Eassa, Charles N. "Enabling Combatant Commander's Ability to Conduct Operations in the Cyber Domain." Master's Thesis, U.S. Army War College, 2012.

Economist. "A cyber-riot: Estonia has faced down Russian Rioters. But its websites are still under attack." *The Economist*, 10 May 2007. http://www.economist.com/node/9163598.

Economist. "North Korean cyber-rattling." *The Economist*, 17 May 2013. http://www.economist.com/blogs/babbage/2013/05/digital-warfare.

Economist. "Responding to Russia's inept bullying." *The Economist*, 10 May 2007. http://www.economist.com/node/9142057.

Eom, Jung-Ho, Nam-Uk Kim, Sung-Hwan Kim, and Tai-Myoung Chun. "Cyber Military Strategy for Cyberspace Superiority in Cyber warfare." *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference.* IEEE: IEEE Xplore Digital Library, 2012: 295-299.

Finextra. "South Korean bank hit by cyber-attack." *Finextra*, 20 April 2011. http://www.finextra.com/News/Fullstory.aspx?newsitemid=22486.

Finkle, Jim. "Researchers say Stuxnet was deployed against Iran in 2007." *Reuters*. 26 February 2013. http://www.reuters.com/article/2013/02/26/us-cyberwar-stuxnet-idUSBRE91P0PP20130226.

Fox, Stuart. "Why Cyberwar is Unlikely." *Tech News Daily*, 2 July 2011. http://www.technewsdaily.com/6962-cyberwar-unlikely-deterrence-cyber-war.html.

Franzese, Patrick W., Lt Col, USAF. "Sovereignty in Cyberspace: Can it Exist?" Air Force Law Review 64, (2009): 1-42.

Goodin, Dan. “Georgian cyber attacks launched by Russian crime gangs: With help from Twitter, Facebook and Microsoft.” *The Register*, 18 August 2009. http://www.theregister.co.uk/2009/08/18/georgian_cyber_attacks/.

Goodin, Dan. “Kremlin-backed youths launched Estonian cyberwar, says Russian official.” *The Register*, 11 March 2009. http://www.theregister.co.uk/2009/03/11/russian_admits_estonian_ddos/.

Gorman, Siobhan, and Julian E. Barnes. “Cyber Combat: Act of War.” *The Wall Street Journal*, 2011. http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html#ixzz1O2urKzzR.

Gostev, Alexander. “The Flame” Questions and Answers.” *Securelist*, 28 May 2012. http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers.

Grant, R.G. *Battle at Sea: 3,000 Years of Naval Warfare*. London: Dorling Kindersley, 2008.

Grauman, Brigid. “Cyber-Security: The Vexed Question of Global Rules.” Brussels, BE: Security & Defense Agenda, 2012.

Gray, Colin S. *Fighting Talk: Forty Maxims on War, Peace, and Strategy.* London: Praeger Security International, 2009. Kindle edition.

Gray, Colin S. *Modern Strategy*. Oxford: Oxford University Press, 1999.

Greenberg, Andy. “Hackers Reveal Nasty New Car Attacks—With Me Behind the Wheel (Video).” *Forbes*, 24 July 2013. http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/.

Greenberg, Andy. “Shopping for Zero-Days: A Price List for Hackers’ Secret Software Exploits.” *Forbes*, 23 March 2012. http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.

Gross, Michael Joseph. “A Declaration of Cyber-War.” *Vanity Fair*, 2011. http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

Gunn, Angela. “An inter-office squabble could have triggered a Baltic cyber-war.” *Betanews*, 11 March 2009. http://betanews.com/2009/03/11/an-inter-office-squabble-could-have-triggered-a-baltic-cyber-war/.

Haig, Zsolt. "Connections Between Cyber Warfare and Information Operations." *AARMS*, Volume 8, No. 2, 2009: 329-337.

Hall, Camilla and Javier Blas. "Aramco cyber attack targeted production." *Financial Times*, 10 December 2012. http://www.ft.com/intl/cms/s/0/5f313ab6-42da-11e2-a4e4-00144feabdc0.html#axzz2dfwhMlKi.

Han, Jane. "Cyber Attack Hits Korea for Third Day." *Korea Times*, 9 July 2009. http://www.koreatimes.co.kr/www/news/biz/2009/09/123_48203.html.

Hansen, Andrew P. "Cyberflag: A Realistic Training Construct." Master's Thesis, Air Force Institute of Technology, 2008.

Hare, Forrest B. and Glenn Zimmerman. "The Air Force in Cyberspace: Five Myths of Cyberspace Superiority." *Military Perspectives on Cyberpower.* Edited by Larry K. Wentz, Charles L. Barry, and Stuart H. Starr. Washington, DC: Center for Technology and National Security Policy, 2009: 87-95.

Hart, Liddell, B. H. *Strategy*. 2nd ed., New York: Penguin Books, 1967.

Hayden, Michael V., General, USAF, Retired. "The Future of Things 'Cyber'." *Strategic Studies Quarterly* 5, no. 1, 2011: 5.

Heiss Online, "DDoS attacks on Estonian web sites using one million hijacked computers." *The H Security*, 18 May 2007. http://www.h-online.com/security/news/item/Russian-youth-movement-claims-to-have-carried-out-cyber-attacks-on-Estonia-740487.html.

Heiss Online, "Russian Youth Movement Claims to have carried out Cyber Attacks." *The H Security*, 12 March 2009. http://www.h-online.com/security/news/item/Russian-youth-movement-claims-to-have-carried-out-cyber-attacks-on-Estonia-740487.html.

Heiss Online, "Student fined for DDoS attack on Estonia." *The H Security*, 25 January 2008. http://www.h-online.com/security/news/item/Student-fined-for-DDoS-attack-on-Estonia-735897.html.

Herskovitz, Jon. "PCs could be hit next in Web attack – South Korea." *Reuters*, 10 July 2009. http://in.reuters.com/article/2009/07/10/idINIndia-40942120090710.

Heuser, Beatrice. *The Evolution of Strategy: Thinking War from Antiquity to the Present.* Cambridge: Cambridge University Press, 2010,

Higgins, Kelly Jackson. "Free 'Active Defense' Tools Emerge." *Security Dark Reading*, 11 July 2013. http://www.darkreading.com/intrusion-prevention/free-active-defense-tools-emerge/240158160.

Higgins, Kelly Jackson. "Nearly One-Fifth of Enterprise Operating Systems not Fully Patched." *Security Dark Reading*, 23 August 2013. http://www.darkreading.com/vulnerability/nearly-one-fifth-of-enterprise-operating/240160403.

Holden. "Cyber Attacks in the Spin Cycle: Saudi Aramco and Shamoon." *Analysis Intelligence*, 1 November 2012. http://analysisintelligence.com/cyber-defense/narrative-of-a-cyber-attack-saudi-aramco-and-shamoon/.

Hsu, Merna H., H. "Gaining and Maintaining Cyberspace Superiority: Quest for a Holy Grail?" Thesis, School of Advanced Air and Space Studies, 2009.

Independent. "S. Korea bank probed over 'cyber-attack' shutdown." *The Independent*, 19 April 2011. http://www.independent.co.uk/life-style/s-korea-bank-probed-over-cyberattack-shutdown-2269767.html.

Information Age. "S Korea accuses N Korea of cyber attack on bank." *Information Age*, 3 May 2011. http://www.information-age.com/technology/security/1621658/s-korea-accuses-n-korea-of-cyber-attack-on-bank.

Infosecurity. "North Korea likely source of DDoS attacks against South Korean sites, says McAfee." *Infosecurity*, 7 July 2011. http://www.infosecurity-us.com/view/19258/north-korea-likely-source-of-ddos-attacks-against-south-korean-sites-says-mcafee/.

Japmarpaung, "Dark Seoul – Postmortem." 3 May 2013. http://japmarpaung.com/2013/05/03/dark-seoul-postmortem/.

Je-hae, Do. "Hackers Yet to be Confirmed." *The Korea Times*, 10 July 2009. http://www.koreatimes.co.kr/www/news/nation/2009/07/116_48267.html.

Kallberg, Jan and Bhavani Thuraisingham. "Cyber Operations: Bridging from Concept to Cyber Superiority." *Joint Force Quarterly*, Issue 68 1st Quarter 2013, 53-58.

Kanellos, Michael. "New Wi-Fi distance record: 382 kilometers." *CNet*, 18 June 2007. http://news.cnet.com/8301-10784_3-9730708-7.html.

Kaplan Dan, "One month after recent Java update, 7 percent of users patched." *SC Magazine for IT Security Professionals*, 5 June 2013. http://www.scmagazine.com/one-month-after-recent-java-update-7-percent-of-users-patched/article/296431/.

Kassner, Michael. “Deep Packet Inspection: What you Should Know.” *ZDNet*, http://www.zdnet.co.uk/news/it-strategy/2008/07/31/deep-packet-inspectionwhat-you-should-know-39454822/.

Keegan, John. *The Second World War*. New York: Penguin, 1989.

Kelley, Olen L. “Cyberspace Domain: A Warfighting Substantiated Operational Environment Imperative.” Master’s Thesis, U.S. Army War College, 2008.

Kim, Jack. “UPDATE 3-More Web attacks hit, North Korea suspected.” *Reuters*, 9 July 2009. http://www.reuters.com/article/2009/07/09/korea-south-internet-idUSPEK47527720090709.

Kim, Sue-young. “Spy Chief Says Cyber Attacks Work of N. Korea.” *The Korea Times*, 23 August 2013. http://www.koreatimes.co.kr/www/news/nation/2010/04/116_54596.html.

Klein, John J. “Corbett in Orbit: A Maritime Model for Strategic Space Theory.” *Naval War College Review* 57, no. 1 (2004): 59-74.

Knickmeyer, Ellen. “After Cyberattacks, Saudi Steps Up Online Security.” *Wall Street Journal*, 25 August 2013. http://blogs.wsj.com/middleeast/2013/08/26/after-cyberattacks-saudi-steps-up-online-security/.

Koo, Soo-Kyung. “Cyber Security in South Korea: The Threat Within.” *The Diplomat*, 19 August 2013. http://thediplomat.com/2013/08/19/cyber-security-in-south-korea-the-threat-within/?all=true.

Korea Times. “Dreadful Cyber War.” *The Korea Times*, 10 July 2009. http://www.koreatimes.co.kr/www/news/opinon/2009/07/137_48261.html.

Korea Times. “N. Korea Operates Cyber War Unit.” *The Korea Times*, 5 May 2009. http://www.koreatimes.co.kr/www/news/nation/2010/04/113_44358.html.

Kramer, Franklin D. “Cyberpower and National Security: Policy Recommendations for a Strategic Framework.” In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 3-23. Washington, DC: Potomac Books, 2009.

Kramer, Franklin D. and Larry K. Wentz “Cyber Influence and International Security.” In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 343-361. Washington, DC: Potomac Books, 2009.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. *Cyberpower and National Security*. 1st ed. Washington, DC: Potomac Books, 2009.

Krebs, Michael. "Cyber attack on U.S., North Korea suspected." *Digital Journal*, 8 July 2009. http://www.digitaljournal.com/article/275587.

Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 24-42. Washington, DC: Potomac Books, 2009.

Kugler, Richard L. "Deterrence of Cyber Attacks." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 309-340. Washington, DC: Potomac Books, 2009.

Kwang, Kevin. "S. Korea, US attacks possibly launched by N. Korea." *ZDNet*, 6 July 2011. http://www.zdnet.com/s-korea-us-attacks-possibly-launched-by-n-korea-2062301087/.

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. "A Brief History of the Internet." http://www.isoc.org/internet/history/brief.shtml.

Lewis, James A. "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats." Center for Strategic & International Studies, 2002.

Lewis, James Andrew. "Neither Mahan nor Mitchell: National Security Space and Spacepower, 1945-2000." In *Toward a Theory of Spacepower: Selected Essays*, edited by Charles D. Lutes, Peter L. Hays, Vincent A. Manzo, Lisa M. Yambrick and M. Elaine Bunn, 277-99. Washington, DC: National Defense University Press, 2011.

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare.* Cambridge: Cambridge University Press, 2007.

Libicki, Martin C. *Cyberdeterrence and Cyberwar.* Santa Monica: RAND Corporation, 2009.

Libicki, Martin C. "Military Cyberpower." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 275-284. Washington, DC: Potomac Books, 2009.

Lonsdale, David J. *The Nature of War in the Information Age.* London: Frank Cass, 2004.

Louis, Meera and Ott Ummelas. "Estonian Premier Says Internet Attacks Not Acceptable (Update2)" *Bloomberg*, 24 May 2007.

http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a9C66FjyCFBk&refer=europe.

Luttwak, Edward, N. *Strategy: The Logic of War and Peace.* Cambridge, MA: Belknap Press, 2003.

MacIsaac, David. "Voices from the Central Blue: The Air Power Theorists." In *Makers of Modern Strategy: From Machiavelli to the Nuclear Age*, edited by Peter Paret, 624-647. Princeton: Princeton University Press, 1986.

Mahan, Alfred T. *The Influence of Sea Power Upon History, 1660-1783*. New York, NY: Dover Publications, 1987.

Mahan, Alfred T. *Mahan on Naval Strategy: Selections from the Writings of Rear Admiral Alfred Thayer Mahan*. Edited by Allan Westcott. Boston: Little, Brown, and Company, 1918.

Mahan, Alfred T. *Mahan on Naval Strategy: Selections from the Writings of Rear Admiral Alfred Thayer Mahan*. Edited by John B. Hattendorf. Annapolis, MD: Naval Institute Press, 1991.

Mahdi, Wael. "Saudi Arabia Says Aramco Cyberattack Came From Foreign States." *Bloomberg*, 9 December 2012. http://www.bloomberg.com/news/2012-12-09/saudi-arabia-says-aramco-cyberattack-came-from-foreign-states.html.

Markoff, John. "Before the Gunfire, Cyberattacks." *The New York Times*, 12 August 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0.

Matrosov, Aleksandr, Eugene Rodionov, David Harley, and Juraj Malcho. "Stuxnet Under the Microscope: Revisions 1.31." *eSeT*. Accessed 25 August 2013. http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

Mauro, Ryan. "Major North Korean Cyber Attack on South." *Frontpage Mag*, 1 September 2011. http://frontpagemag.com/2011/ryan-mauro/major-north-korean-cyber-attack-on-south/.

McAfee. "Ten Days of Rain: Expert analysis of distributed denial-of-service attacks targeting South Korea." White Paper developed by McAfee Security. 2011.

McCarthy, Thomas David. "Traveling Domain Theory: A Comparative Approach for Cyberspace Theory Development." PhD Dissertation, Fletcher School of Law and Diplomacy, 2012.

McDermott, Roger N. "Russia's Conventional Armed Forces and the Georgian War." *Parameters*, Spring 2009, 65-80.

McKee, Kandice. “A Review of Frequently Used Cyber Analogies.” Smithfield, VA: National Security Cyberspace Institute, 2011.

Miller, James N., Dr. “Statement of Dr. James N. Miller Principal Deputy Under Secretary of Defense for Policy.” In Hearing on the Department of Defense in Cyberspace and U.S. Cyber Command, edited by U.S. Congress (House of Representatives) Committee on Armed Services Subcommittee on Emerging Threats and Capabilities. Washington, DC, 2011.

Miller, Robert A., and Daniel T. Kuehl. “Cyberspace and the ‘First Battle’ in 21stcentury War.” *Defense Horizons* 68, 2009: 6.

Mitchell, William. *Winged Defense: The Development and Possibilities of Modern Air Power, Economic and Military*. Mechanicsburg, PA: Stackpole Books 1925. Reprint, 1999.

Mogg, Trevor. “Smart Toilet Security Flaw Could Result in Nasty Surprise.” *Fox News*, 5 August 2013. http://www.foxnews.com/tech/2013/08/05/smart-toilet-security-flaw/.

Molander, Roger C., Andrew S. Riddile and Peter A. Wilson. *Strategic Information Warfare: A New Face of War*. Santa Monica, CA: RAND, 1996.

Montalbano, Elizabeth. “DOD Website Sells Public On Cybersecurity Strategy.” *Informationweek*, 2011. http://www.informationweek.com/news/government/security/231002588#.

Moya, Jared. “Massive DDoS attacks target Estonia; Russia accused.” *Zeropaid*, 14 May 2007. http://www.zeropaid.com/news/8759/massive_ddos_attacks_target_estonia_russia_accused/.

Musashi, Miyamoto. *The Book of Five Rings*. Start Publishing LLC, 2012. Kindle edition.

Mysinchew. “S. Korea to step up security against cyber attacks.” *Mysinchew*, 24 May 2011. http://www.mysinchew.com/node/57802.

Nakashima, Ellen. “An army of tech-savvy warriors has been fighting its battles in cyberspace.” *The Washington Post*, 24 September 2010, A18.

Nakhlawi, Elham, Mustafa Al Arab, Caroline Faraj, Tess Eastment, Aneesh Raman and Brad Lendon. “Third undersea Internet cable cut in Mideast.” *Cable News Network*, 1 February 2008. http://www.cnn.com/2008/WORLD/meast/02/01/internet.outage/.

Naraine, Ryan. "Shodan search engine exposes insecure SCADA systems." *ZDNet*, 2 November 2010. http://www.zdnet.com/blog/security/shodan-search-exposes-insecure-scada-systems/7611.

"National Security Strategy of the United States 2010." edited by White House, 2010.

"National Security Strategy of the United States 2013 (Draft)." edited by White House, 2013. http://www.utexas.edu/lbj/sites/default/files/file/news/National%20Security%20Strategy%202013%20%28Final%20Draft%29.pdf.

New York Times. "A cyberblockade in Estonia." *The New York Times*, 3 June 2007. http://www.nytimes.com/2007/06/03/opinion/03iht-edestonia.1.5976188.html?_r=1&.

Ngak, Chenda. "The 25 most common passwords of 2012." *CBS News*, 24 October 2012. http://www.cbsnews.com/8301-205_162-57539366/the-25-most-common-passwords-of-2012/.

Nicloa, Stefan. "The World's First Internet War." *UPI*, 6 August 2007. http://www.spacedaily.com/reports/The_World_First_Internet_War_999.html.

O'Harrow, Robert. *Zero Day: The Threat in Cyberspace.* New York: Diversion Books, 2013. Kindle edition.

O'Neil, William D. "Cyberspace and Infrastructure." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 113-146. Washington, DC: Potomac Books, 2009.

Organization for Economic Co-operation and Development. "Global Commons Definition." 2011. http://unstats.un.org/unsd/environmentgl/gesform.asp?getitem=573.

Owens, William A., Kenneth W. Dam, and Herbert S. Lin, eds. Technology, *Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Edited by National Research Council. Washington, DC: National Academies Press, 2009.

Pape, Robert. *Bombing to Win: Air Power and Coercion in War.* London: Cornell University Press, 1996.

Peritz, Aki J. and Michael Sechrist. "Protecting Cyberspace and the US National Interest." Harvard Kennedy School Belfer Center for Science and International Affairs, 2010.

Perlroth, Nicole. "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back." *The New York Times*, 23 October 2012. http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all.

Poulsen, Kevin. "Estonia 'Cyberwar' Wasn't." *Wired*, 1 June 2007. http://www.wired.com/threatlevel/2007/06/estonia_cyberwa/

Preatoni, Roberto. "The digital bending of Estonia on its physical knees: The Lessons we are NOT going to learn." Mi2g ATCA, 2 June 2007. http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/020607.php

Ratcliff, R., A. *Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers*. Cambridge: Cambridge University Press, 2006.

Rattray, Gregory J. "An Environmental Approach to Understanding Cyberpower." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 253-274. Washington, DC: Potomac Books, 2009.

Redden, Michael E. and Michael P. Hughes. "Defense Planning Paradigms and the Global Commons" in *Joint Forces Quarterly*, Issue 60 (1st Quarter 2011), 61-66.

Reuters. "Aramco Says Cyberattack Was Aimed at Production." *New York Times*, 10 December 2012. http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0.

Reuters. "Estonia to bolster cyber defenses after attacks." *Reuters*, 5 July 2007. http://www.reuters.com/article/2007/07/05/us-estonia-cyberattack-idUSL0588580120070705.

Reuters. "N. Korea rejects South charge it was behind bank cyber attack." *Reuters*, 15 May 2011. http://in.reuters.com/article/2011/05/15/idINIndia-57024320110515.

Reuters. "North Korea behind cyber attack on S. Korea bank – prosecutors." *Reuters*, 3 May 2011. http://in.reuters.com/article/2011/05/03/idINIndia-56736320110503.

Reuters. "Pro-Kremlin Activist Claims Responsibility for Estonia Cyberattack." *Fox News*, 13 March 2009. http://www.foxnews.com/story/2009/03/13/pro-kremlin-activist-claims-responsibility-for-estonia-cyberattack/.

Rogers, John C. "Shaping the Air Force Operational Environment in Cyberspace." Air War College, 2009.

Rosenzweig, Paul. *How Conflicts in Cyberspace are Challenging America and Changing the World.* Santa Barbara, CA: Praeger, 2013. Kindle edition.

SANS. "Intrusion Detection Systems: Definition, Need and Challenges." *SANS*, 2001. http://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-systems-definition-challenges-343.

Sang-Hun, Choe. "Computer Networks in South Korea Are Paralyzed in Cyberattacks." 20 March 2013. http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html.

Sanger, David E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power.* New York: Broadway Books, 2013. Kindle edition.

Sanger, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran." *The New York Times.* 1 June 2012.

Sanger, David E., David Barboza and Nicole Perlroth. "Chinese Army Unit Is Seen as Tied to Hacking Against U.S." *New York Times*, 19 February 2013. http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all&_r=2&.

Saudi Gazette. "PCs could be hit." *The Saudi Gazette,* 22 August 2013. http://www.saudigazette.com.sa/index.cfm?method=home.regcon&contentid=20090071143350.

Scarborough, Rowan. "In classified cyberwar against Iran, trail of Stuxnet leak leads to White House." *The Washington Times,* 18 August 2013.

Schelling, Tom, *Arms and Influence.* New Haven: Yale University Press, 1996.

Security Focus. "Georgian cyber attackers only civilians, report says." *Security Focus*, 18 August 2009. http://www.securityfocus.com/brief/998

Shachtman, Noah. "Kremlin Kids: We Launched the Estonian Cyber War." *Wired*, 11 March 2009. http://www.wired.com/dangerroom/2009/03/pro-kremlin-gro/.

Shakarian, Paulo. "Stuxnet: Cyberwar Revolution in Military Affairs." *Small Wars Journal*, 15 April 2011.

Shakarian, Paulo. "The 2008 Russian Cyber Campaign Against Georgia." *Military Review*, November-December 2011, 63-68.

Shakarian, Paulo, Jana Shakarian and Andrew Ruef. *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. Amsterdam: Syngress, 2013. Kindle edition.

Shanker, Thom and David E. Sanger. "U.S. Suspects Iran Was Behind a Wave of Cyberattacks." *New York Times*, 13 October 2012. http://www.nytimes.com/2012/10/14/world/middleeast/us-suspects-iranians-were-behind-a-wave-of-cyberattacks.html?_r=2&pagewanted=all.

Sherstobitoff, Ryan and Itai Liba. "Dissecting Operation Troy: Cyberespionage in South Korea." White Paper developed by McAfee Labs. 2013.

Shipp, Jac W. "Space and Cyberspace: The Overlap and Intersection of Two Frontiers." *Army Space Journal*, Spring-Summer 2011, 40-43.

Smith, Jeffrey G. Jr. "A Unified Field Theory for Full-Spectrum Operations: Cyberpower and the Cognitive Domain." In *Military Perspectives on Cyberpower.* Edited by Larry K. Wentz, Charles L. Barry, and Stuart H. Starr. Chapter 2, 29-71. Washington, DC: Center for Technology and National Security Policy, 2009.

Sridharan, Vasudevan. "3,000 North Korean Hackers in 'Trolling' War Against Seoul." *International Business Times*, 13 August 2013. http://www.ibtimes.co.uk/articles/498746/20130813/north-korea-cyber-attack-pyongyang-kim-jongun.htm.

Strassler, Robert B. ed. *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*. New York: Touchstone, 1996.

Sullivan, Sean. "Stuxnet Redux: Questions and Answers." *F-Secure*, 23 November 2010. http://www.f-secure.com/weblog/archives/00002066.html.

Sun Tzu. *The Art of War.* Trans by Samuel B. Griffith with Forward by B. H. Liddell Hart. Oxford University Press: Oxford, 1971.

Thawte. "Cyberattack Traced to North Korea." *Thawte*, 2013. http://www.thawte.com/about/news/?story=423684.

TRADOC Pamphlet 535-7-8. *The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028*, 22 February 2010.

Treat, Tim. "The Way Ahead for Cyberspace Operations: A JTIDS Analysis." Master's Thesis, Air Force Institute of Technology, 2007.

Trias, Eric D. and Brian M. Bell. "Cyber This, Cyber That…So What?" *Air Space Power Journal*, Volume 24, no. 1 (2010): 90-100.

United Nations. *United Nations Convention on the Law of the Sea.* 1994. http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.

U.S. Cyber Consequences Unit. "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008." US-CCU Special Report, August 2009.

U.S. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace.* Washington, DC: U.S Government Printing Office, 2011.

U.S. Department of Defense, Joint Chiefs of Staff. "Department of Defense Dictionary of Military Associated Terms Joint Publication 1-02." Washington DC: Government Printing Office, 2010, as amended through 15 December 2012.

U.S. Department of Defense, Joint Chiefs of Staff. "Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate." in *Joint Force Quarterly* issue 67. Washington, DC: Government Printing Office, 2012.

U.S. Department of Defense, Joint Chiefs of Staff. Joint Operations. Vol. 3-13, *Information Operations.* Washington, DC: U.S Government Printing Office, 2012.

U.S. Department of Defense, Joint Chiefs of Staff. "The National Military Strategy for Cyberspace Operations." edited by Chairman Joint Chiefs of Staff. Washington, DC, 2006.

U.S. Department of Defense, U.S. Joint Forces Command. "Joint, Techniques, and Procedures: Assessment of Joint Operations." 10 March 2008.

U.S. President. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World." 30. Washington, DC, 2011.

Valeriano, Brandon and Ryan Maness. "Cyberwar and Rivalry: The Dynamics of Cyber Conflict between Antagonists, 2001-2011." *Western Political Science Association*, 2012. http://wpsa.research.pdx.edu/meet/2012/manessvaleriano.pdf.

Van Evera, Stephen. *Guide to Methods for Students of Political Science.* Ithaca, NY: Cornell University Press, 1997.

Wahab, Siraj. "Cyber Attack on Aramco A 'Global Plot', says Saudi Arabia." *Arab News*, 10 December 2012. http://www.eurasiareview.com/10122012-cyber-attack-on-aramco-a-global-plot-says-saudi-arabia/.

Warden, John. "The Enemy as a System." *Air and Space Power Journal*, 1995, 41-55.

White House. "The Comprehensive National Cybersecurity Initiative." Accessed on 30 August 2013. http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

Whittaker, Zack. "Flame: 'Most complex' cyber-attack ever discovered" *ZDNet*, 28 May 2012. http://www.zdnet.com/blog/btl/flame-most-complex-cyber-attack-ever-discovered/78325.

Wilson, Tim. "Study of Russia-Georgia Cyber Conflict Brings Warnings To U.S. Businesses, Citizens." *Darkreading*, 18 August 2009. http://www.darkreading.com/security/cybercrime/showArticle.jhtml?articleID=219400367&cid=nl_DR_DAILY_T

Wylie, J. C. *Military Strategy: A General Theory of Power Control*. New Brunswick, N.J.: Rutgers University Press, 1967.

Wynne, Michael W. "Flying and Fighting in Cyberspace." *Air Space Power Journal*, Volume 21, no. 1 (2007): 5-9.

Yonhap News Agency. "N. Korea claims Seoul making up stories to raise tension." *Yonhap*, 4 May 2011. http://english.yonhapnews.co.kr/national/2011/05/04/91/0302000000AEN20110504010700315F.HTML.

Yonhap News Agency. "S. Korea seeks int'l cooperation for further probe into cyber attack on bank." *Yonhap*, 15 May 2011. http://english.yonhapnews.co.kr/national/2011/05/15/25/0301000000AEN20110515002500320F.HTML.

Zimet, Elihu and Charles L. Barry. "Military Service Cyber Overview." In *Military Perspectives on Cyberpower.* Edited by Larry K. Wentz, Charles L. Barry, and Stuart H. Starr. Chapter 1, 1-27. Washington, DC: Center for Technology and National Security Policy, 2009.